HEALTH AFFAIRS

TRICARE
Management
Activity

HIPAA Risk Management Activities

HIPAA Training: Summer Sessions

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations. It is intended solely for the use and information of the Military Health System.

HIPAA Risk Management Activities

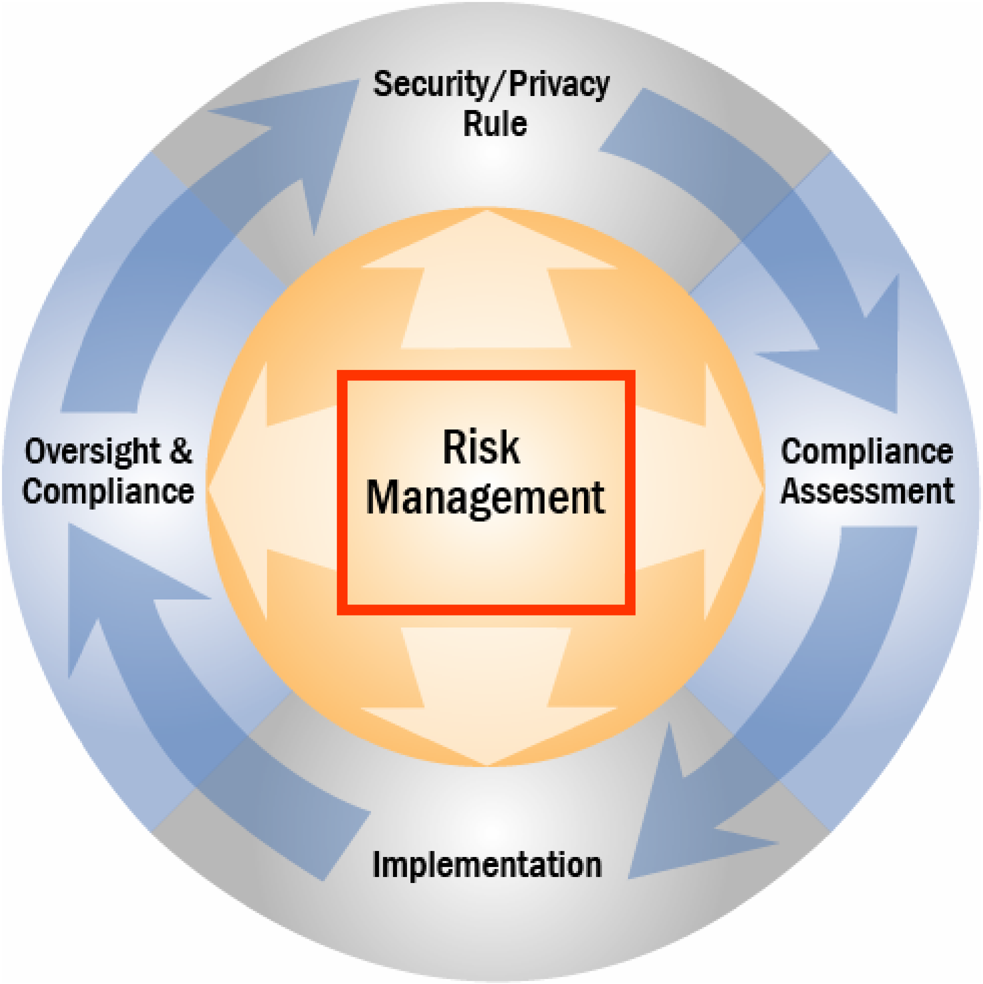
Agenda

- Information Security Concepts
- Risk Management
- Risk Assessment
- Risk Mitigation
- Risk Monitoring
- Risk Management and HIPAA Security
- OCTAVE Methodology vs. NIST Risk Management Approach
- OCTAVE Support for HIPAA Security
- OCTAVE and HIPAA BASICS

Objectives

- After completing this course, you should be able to
  - Define basic information security concepts
  - Describe the elements of the risk management process
  - Identify the risk management activities of the HIPAA Security Rule
  - Describe how OCTAVE and HIPAA BASICS support HIPAA compliance

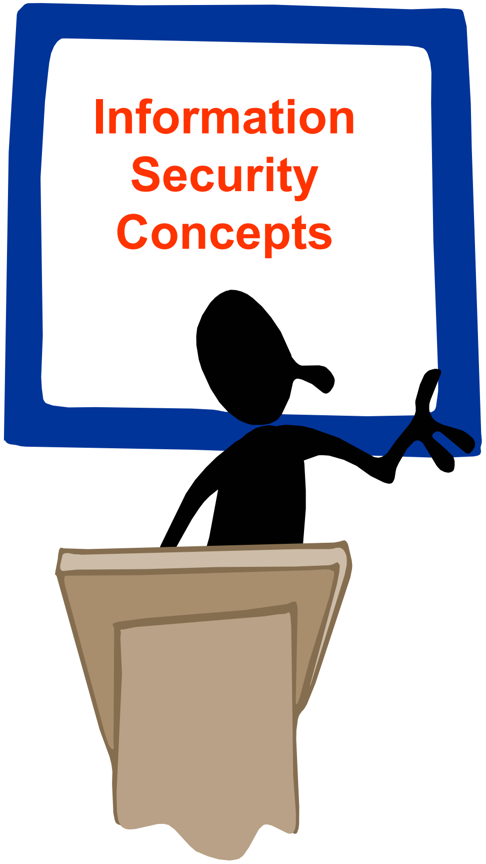
HIPAA Implementation Life Cycle



Information Security Concepts

Information Security Concepts

Objectives



- After completing this module, you should be able to
  - Define terminology and basic concepts of information security
  - Identify the federal regulatory aspects of information security including laws and guidance

Information Security

Information security is achieved through an integrated system of policies, procedures, products, and people that identify, control, and protect information from unauthorized disclosure and by an information protection strategy that is authorized by management and integral to good business practice.

Information Security Concepts

Legislative Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - Office of Management and Budget (OMB) Circular A-123
  - Computer Security Act of 1987
  - OMB Circular A-130, Appendix III
  - Federal Information Security Management Act (FISMA)
  - Federal Managers Financial Integrity Act of 1982 (FMFIA)
  - Government Performance and Results Act (GPRA)

Information Security Concepts

DoD Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - DoD 5000.1-D, Defense Acquisitions
  - DoD 5000.2-R, Mandatory Procedures for MDAS & MAIS Acquisition
  - DoD 5160.54-D, Critical Asset Assurance Program
  - DoD 5200.2-D, Personnel Security Program
  - DoD 5200.2-R, Personnel Security Program
  - DoD 5200.40-I, DITSCAP
  - DoD 5200.8-D, Security of DoD Installations & Resources
  - DoD 5200.8-R, Physical Security Program
  - DoD 5215.2-I, Computer Security Technical Vulnerabilities Reporting Program
  - DoD 6510.18-R, DoD Health Information Privacy
  - DoD 8000.1-D, Defense Information Management Program

DoD Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - DoD 8000.1-D, Defense Information Management Program
  - DoD 8500.1-D, Information Assurance
  - DoD 8500.2-I, Information Assurance Implementation
  - DoD 8510.1-M, DITSCAP
- Service-specific regulations

Information Security Concepts

Security Goals (1 of 2)

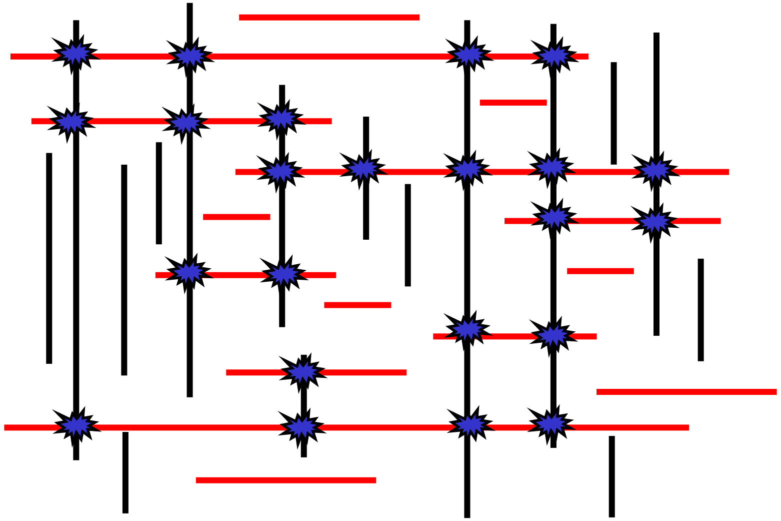
- **Confidentiality** - protecting information from disclosure to unauthorized people or processes
- **Availability** - protecting information and resources from unauthorized or malicious use so the information or resources are accessible when needed

Security Goals (2 of 2)

- **Integrity** - assuring the reliability and accuracy of information and IT resources
- **Authentication -** means for validating a transmission, message or originator
- **Non-repudiation** - providing assurance as to proof of origin and proof of delivery so neither party can deny having processed the data

What is Risk?

- A function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization



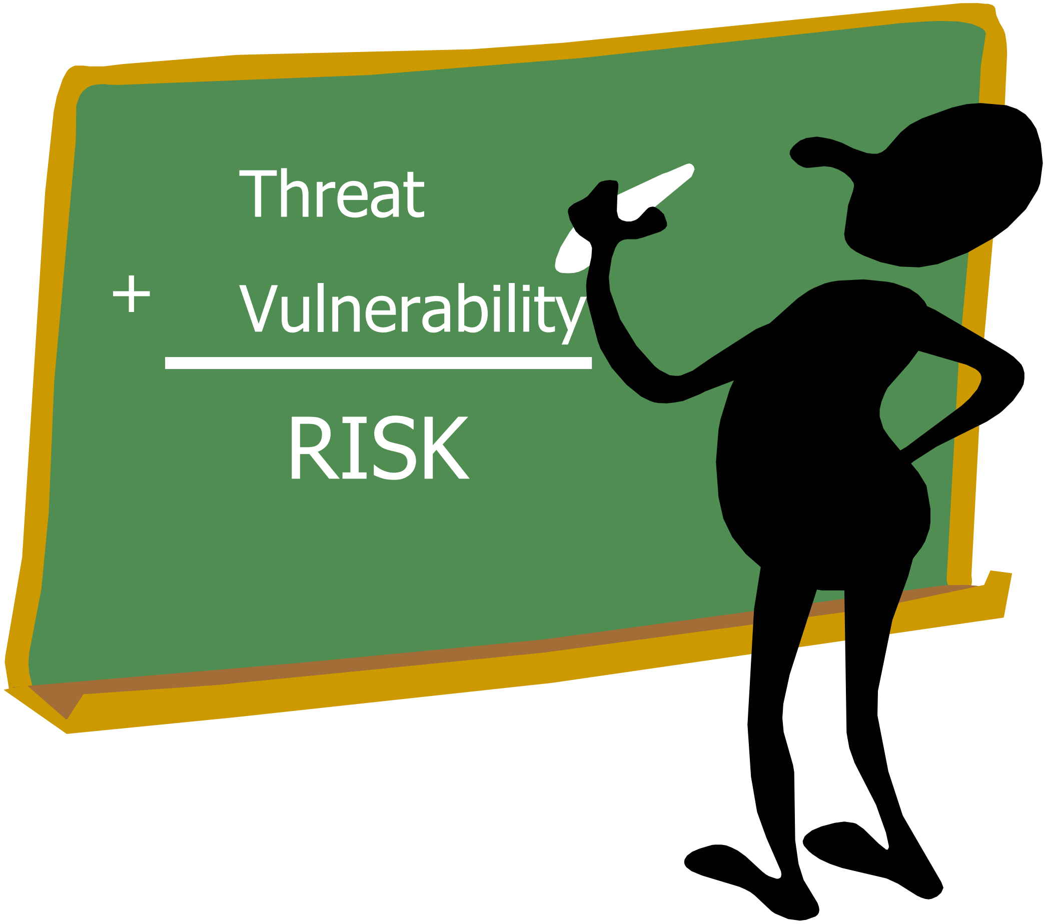
Key:

| Threats

— Vulnerabilities

✸ Risks

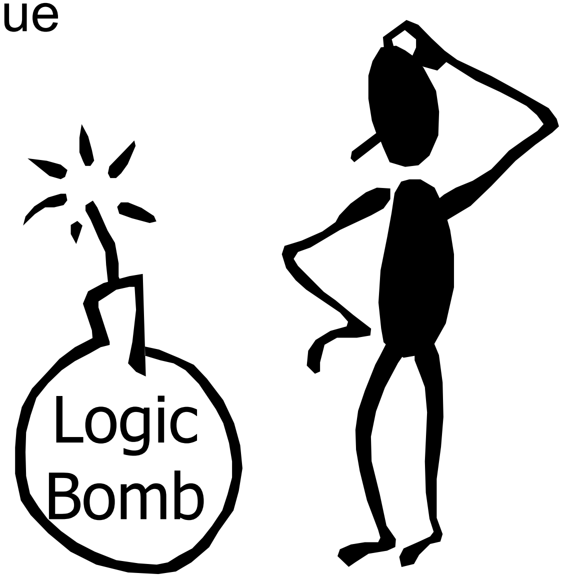
Components of Risk



Threat

- A threat is the potential to cause unauthorized disclosure, changes, or destruction of an asset
  - Unauthorized disclosure = breach of confidentiality
  - Unauthorized changes = integrity failure
  - Unauthorized destruction = availability issue

- Types of threats:
  - Natural
  - Manmade
  - Environmental



Information Security Concepts

Vulnerability

- Any flaw or weakness that can be exploited and results in a breach or a violation of the organization’s security policy

- Types of vulnerabilities:
  - Poorly communicated or implemented policy
  - Poorly trained personnel
  - Misconfigured systems or controls
  - Lack of access controls
  - Lack of physical controls
  - Lack of visitor policy

Information Security Concepts

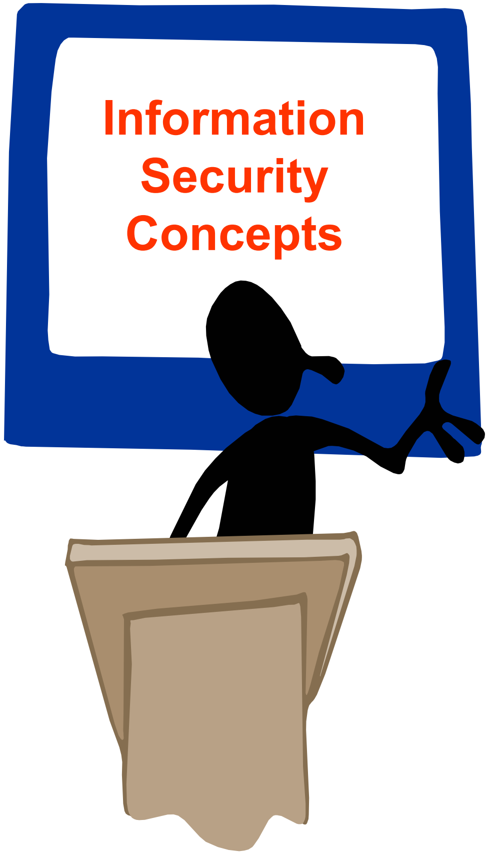
Security Controls

- Categories
  - Administrative
  - Physical
  - Technical

- Sources
  - DoD 8500.2, Information Assurance Implementation
  - Individual Service Regulations
  - NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
  - NIST SP 800-53, Recommended Security Controls for Federal Information Systems (DRAFT)
  - HIPAA Security Rule

Information Security Concepts

Summary



- You should now be able to:
  - Define terminology and basic concepts of information security
  - Identify the federal and DoD regulatory aspects of information security including laws and guidance

Risk Management

Objectives

- After completing this module, you will be able to:
  - List some recent events that highlight the necessity for good risk management practices
  - Identify the three components of risk management

Risk Management

Recent Events (1 of 3)

- **Computer Virus Damage**

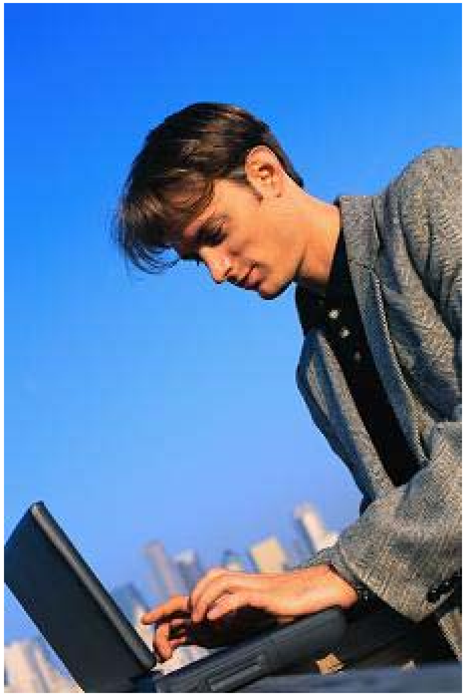
Year	Code Name	Worldwide Economic Impact ($US)
2003	SQL Slammer	$1.0 Billion
2001	Nimda	$653 Million
2001	Code Red(s)	$2.62 Billion
2001	SirCam	$1.15 Billion
2000	Love Bug	$8.75 Billion
1999	Melissa	$1.10 Billion
1999	Explorer	$1.02 Billion

Source: Computer Economics

Risk Management

Recent Events (2 of 3)

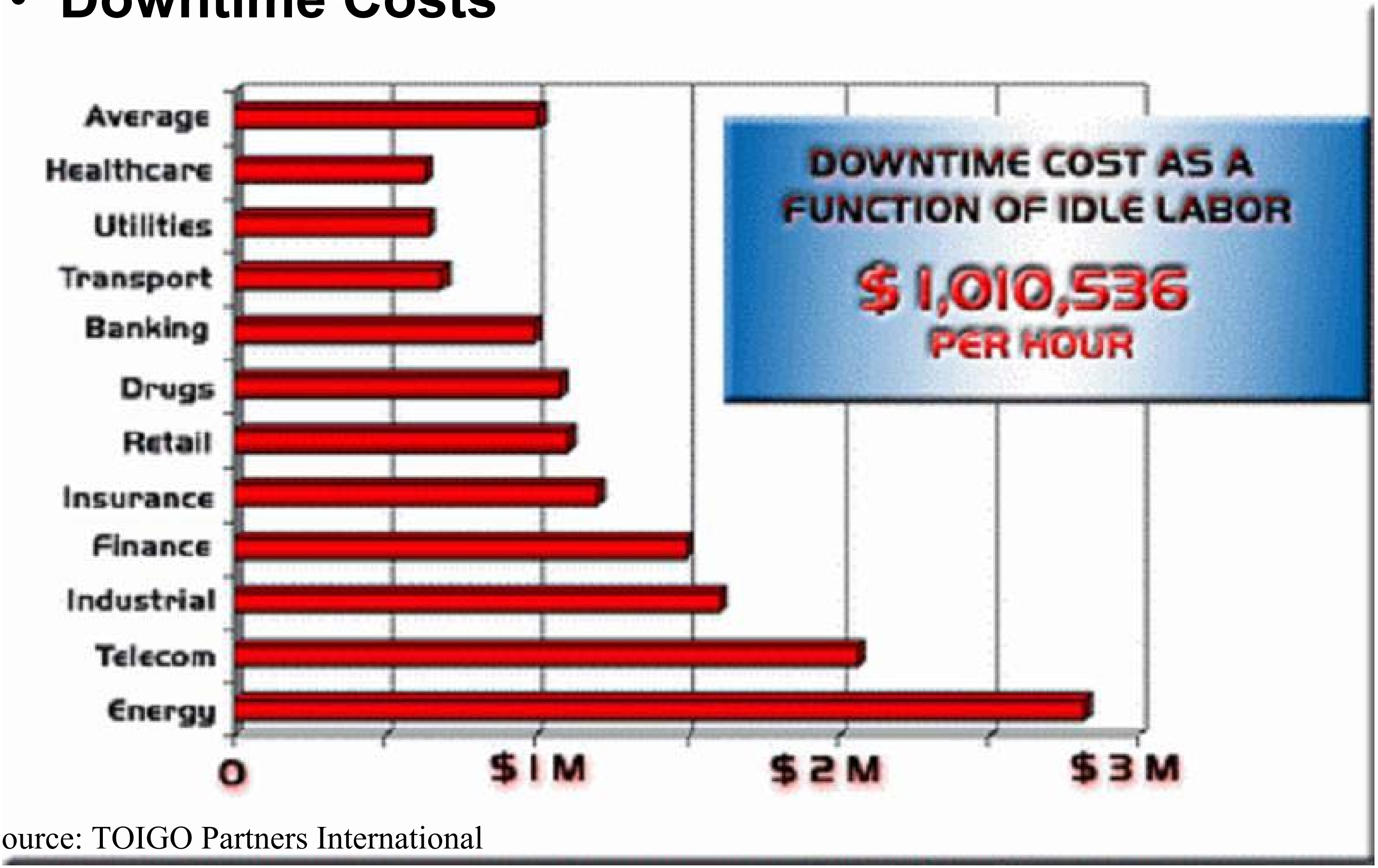
- **Identity Theft**
  - 27 Million Americans – last five years
  - 10 Million Americans – last year
  - Business cost - $47.6 Billion
  - Victim cost - $5.0 Billion



Risk Management

Recent Events (3 of 3)

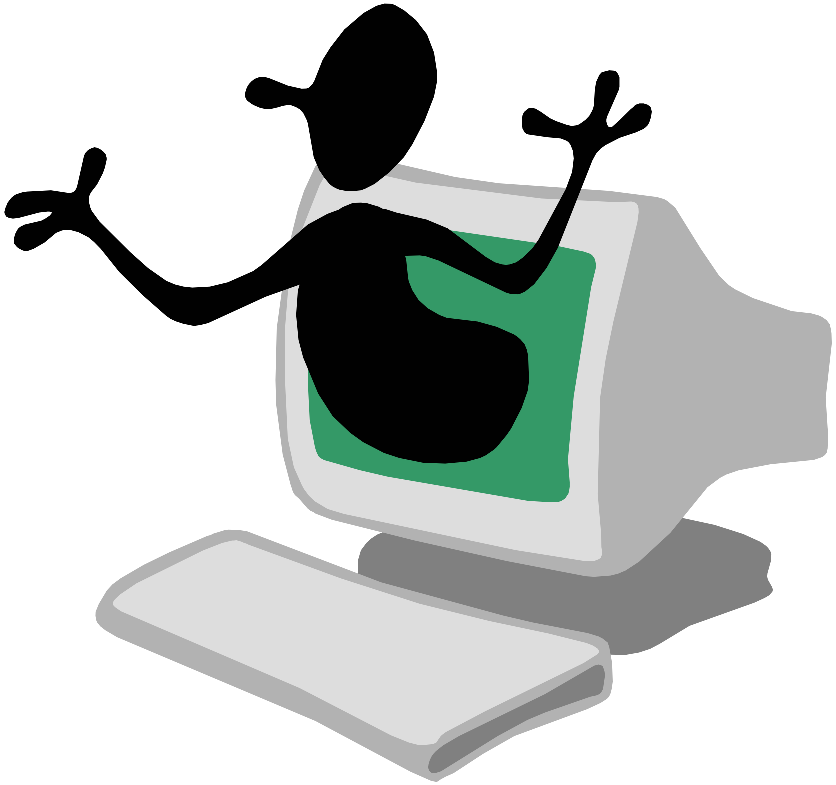
- **Downtime Costs**



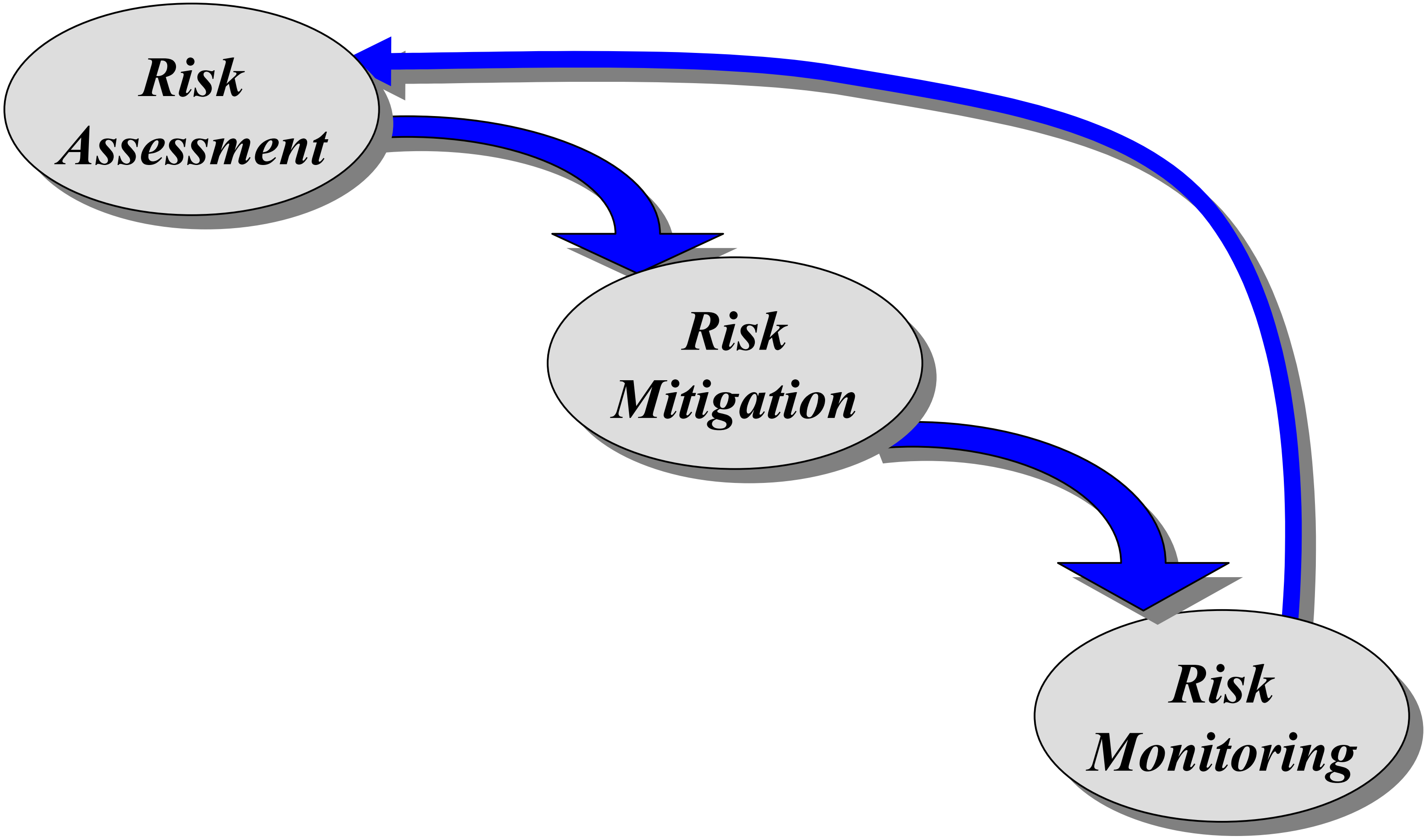
Source: TOIGO Partners International

What is Risk Management?

- Risk Management is composed of three parts:
  - Risk Assessment
  - Risk Mitigation
  - Risk Monitoring



Risk Management Process



Risk Assessment

Risk Mitigation

Risk Monitoring

Summary

- You should now be able to:
  - List some recent events that highlight the necessity for good risk management practices
  - Identify the three components of risk management

Risk Assessment

Risk Assessment

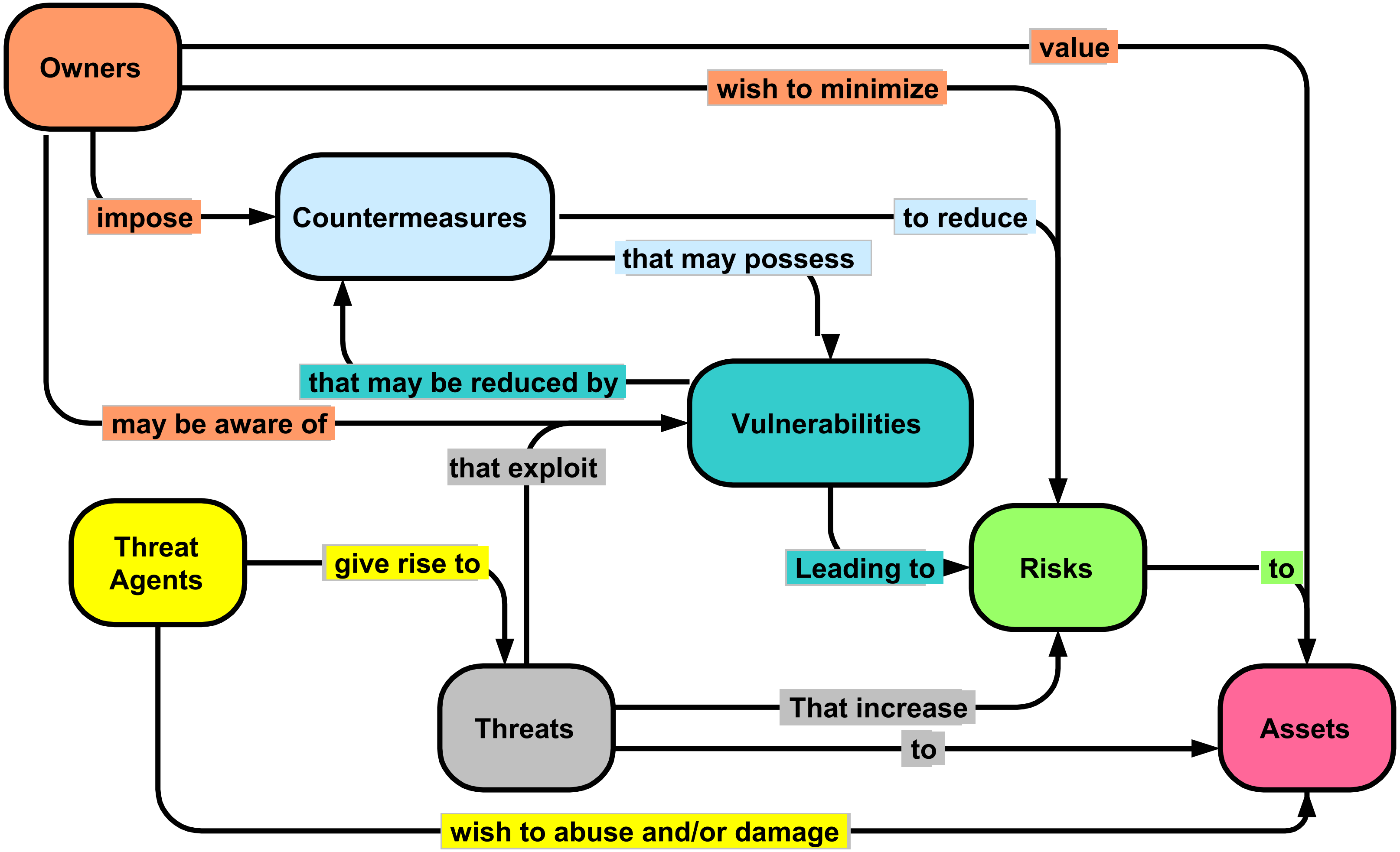
Objectives

- After completing this module, you should be able to:
  - Describe risk assessment
  - Define threats
  - List and describe the nine-steps of the risk assessment methodology

Risk Assessment

- Identification and evaluation of risks and risk impacts
- Recommendations of risk-reducing measures

Risk Assessment Model



Risk Assessment Methodology

- Provides a straightforward description of the system and a qualitative assessment of the risk (e.g., high, moderate, low)

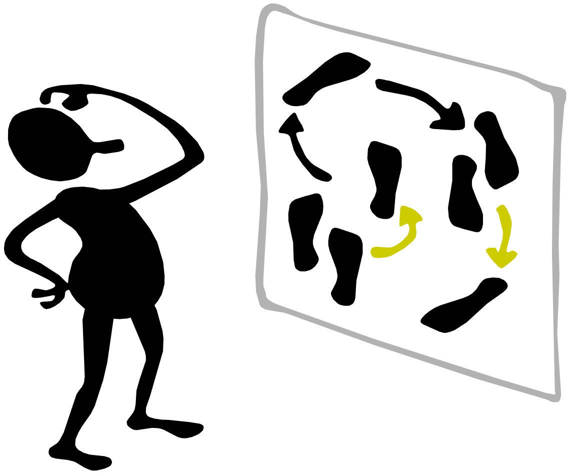
- Risk assessment is composed of a nine-step systematic process
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation

Risk Assessment

Details of the Process

- Steps indicate a general sequence of activities, but some elements of one activity may be mixed with other activities

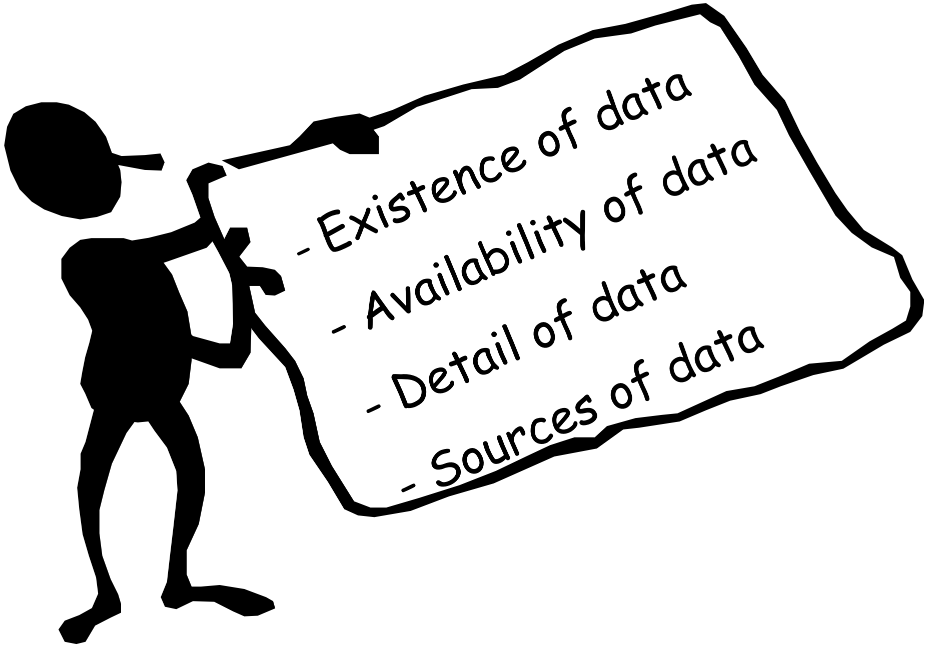
- Activities can also be affected by the system development life cycle phase



Risk Assessment

System Development Life Cycle (SDLC)

- Determines



- Used to assess risk

Risk Assessment

SDLC Phases (1 of 2)

- Initiation
  - Supports the development of a system security policy and security concept of operations (CONOPs)
- Development and Acquisition
  - Supports the security analyses that lead to architecture and design trade offs
- Implementation
  - Supports the assessment of the system implementation against its requirements and within its modeled operation environment

Risk Assessment

SDLC Phases (2 of 2)

- Operation and Maintenance
  - Supports analysis of the system's security posture in the true operational environment
  - Well-defined system hardware and software characteristics and vulnerabilities can be specifically defined and in fact, may be well-known
- Disposal
  - Remove and/or archive information
  - Sanitize hardware and software
  - Ensure proper disposal of all devices

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – System Characterization

Purpose

- To identify system resources and information that constitute the system and its boundaries, including
  - Hardware
  - Software
  - Biomedical Devices
  - System Interfaces
  - Data and Information
  - People
  - System Mission
- Provides the foundation for the remaining steps of the risk assessment process

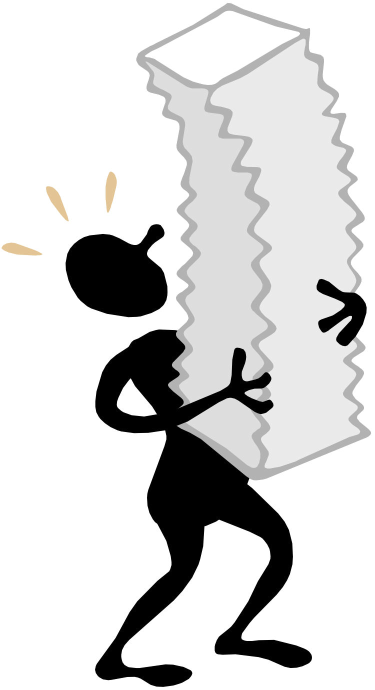
Risk Assessment – System Characterization

Typical Information Sources

- Questionnaires
- Site visits
- Interviews
- Automated scanning tools
- Security documentation
- System and site documentation

Risk Assessment – System Characterization

System and Site Documentation



- Mission statements
- Concept of Operations
- Security policies and procedures
- System functional requirements
- System architectural design documents
- Site operations manual
- Standard operating procedures
- Reports from previous risk assessments
- Physical security plans
- Site floor maps

Risk Assessment – System Characterization

Summary

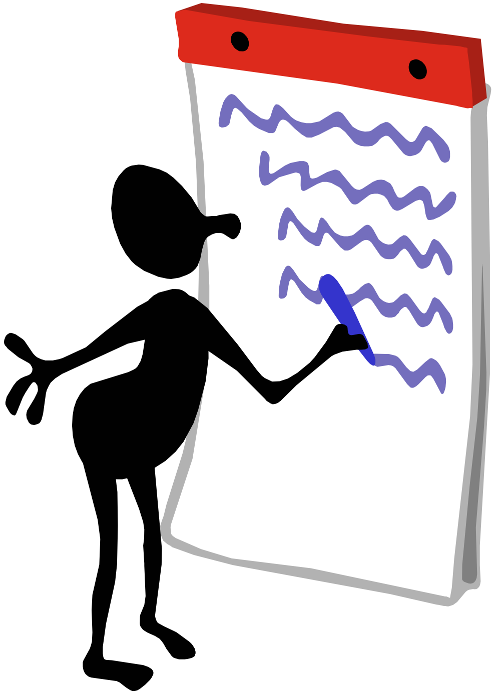
- Purpose of Step One, System Characterization:
  - To identify system resources and information that constitute the system and its boundaries

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Threat Identification

Purpose



- To identify and develop a list of realistic natural, manmade, and environmental threats

Risk Assessment – Threat Identification

Threat Concepts

- Threat
  - The potential to cause unauthorized disclosure, unauthorized modification, or destruction of or denial of access to an asset
- Threat-Source
  - Any circumstance or event with potential to cause harm to an IT system and its assets
  - The common threat-sources can be natural, environmental, or manmade

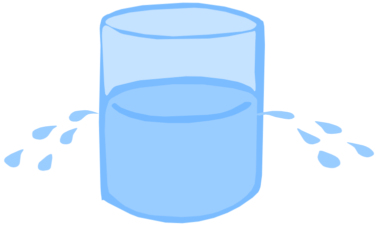
Risk Assessment – Threat Identification

Threats

- Natural
  - Floods
  - Earthquakes
  - Tornadoes
  - Electrical Storms

- Manmade
  - Disgruntled employee
  - Arson
  - Social Engineering
  - Unintentional alterations

- Environmental
  - Long-term power failure
  - Pollution
  - Chemicals
  - Liquid Leakage



Risk Assessment – Threat Identification

Assessment of Threat

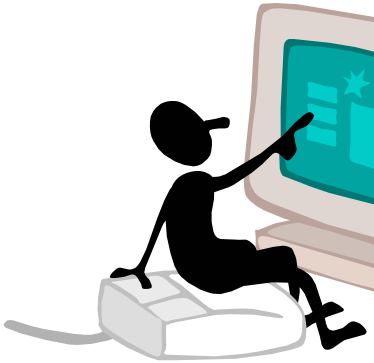
M ~ O ~ M

- Means
- Opportunity
- Motivation – for intentional actions *of your adversaries*

Risk Assessment – Threat Identification

Threat Data Sources

- Many sources of data
  - US-CERT
  - DoD-CERT
  - CERT Coordination Center
  - IAVA
  - Mass media
  - sans.org



- NOTE: Simply because a threat is listed does not necessarily mean that the threat can affect the system

Risk Assessment – Threat Identification

Summary

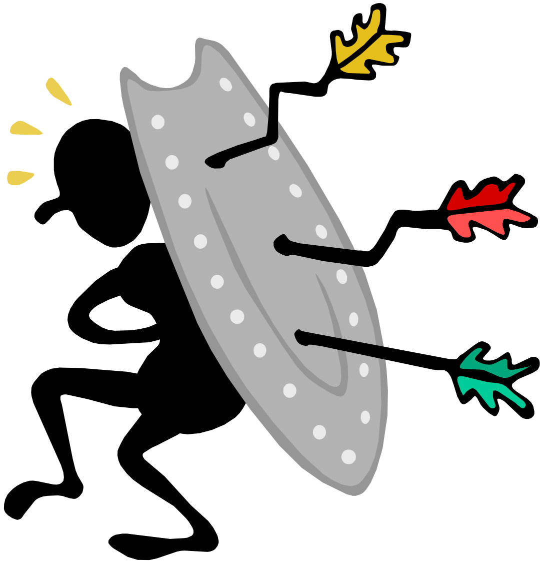
- The outcome of Step 2, Threat Identification will be a threat statement that lists realistic natural and manmade threats and threat agents applicable to the system being evaluated

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Vulnerability Identification

Purpose



- To identify and develop a comprehensive list of possible vulnerabilities that could be used in an attack on the system

Risk Assessment – Vulnerability Identification

What is a Vulnerability?

- Any weakness that can be exploited to gain access to an asset

If an adversary cannot take advantage of the vulnerability, is there a risk?

Risk Assessment – Vulnerability Identification

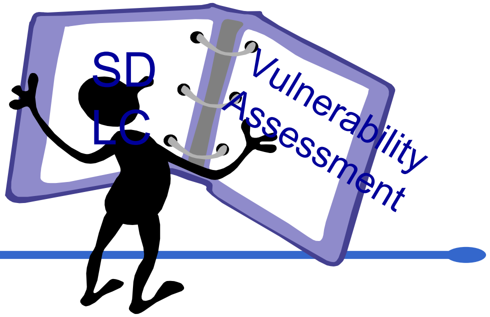
Identifying Vulnerabilities

- Physical security
- Computer/technical security
- Communications security
- Personnel security
- Administrative/Management security

Note: Unmet security requirements are vulnerabilities

Risk Assessment – Vulnerability Identification

Note….



- The phase of the SDLC affects the vulnerability assessment:
  - Initiation

    The primary sources of vulnerabilities are derived from information about the considered or proposed network components, their operating systems and applications
  - Development and Acquisition

    Vulnerability identification expands to include automated tools and databases of known vulnerabilities to identify appropriate system security configurations
  - Operation and Maintenance

    Vulnerability identification includes determining and analyzing implemented security features using:
    - Proactive methods
    - Documented vulnerability sources

Risk Assessment – Vulnerability Identification

Proactive Methods

- Automated vulnerability scanning
- Network mapping
- Security testing and evaluation
- Penetration testing

Risk Assessment – Vulnerability Identification

Documented Sources

- Previous risk assessments
- CERT and CIAC bulletins
- Vendor advisories
- Vulnerability listings
- System software security analyses
- System information analyses
- System development test procedures
- System test results
- System anomaly reports

Risk Assessment – Vulnerability Identification

Also…

- Security requirements collected in Step 1 are reviewed to determine if they are being met by security countermeasures that are either in place or planned

Risk Assessment – Vulnerability Identification

What do you think? Threats vs. Vulnerabilities

Threat or Vulnerability	Answer
1. The LAN is not protected by a firewall.	
2. A malicious user could attempt to gain unauthorized access to the system.	
3. A risk assessment has not been conducted every three years.	
4. The operating system (e.g., Windows NT) allows unlimited bad logon attempts.	
5. Motivated threat agents seeking personal profit gain unauthorized access to the LAN.	
6. Authorized users can use system knowledge to circumvent computer security protective measures, exceed their authorized access privileges, and browse confidential files.	
7. An unauthorized user could disclose, alter, or delete critical and sensitive agency information.	
8. Unnecessary services are running on critical servers.	
9. There is no formal process for removing inactive user accounts and terminated employee system access.	
10. The router access control list allows unrestricted access to the LAN.	

Risk Assessment – Vulnerability Identification

Activity

Identify common threats and vulnerabilities in various medical facility locations

Risk Assessment – Vulnerability Identification

Summary

- During Step 3, vulnerabilities that could be used in an attack on the system are identified and developed into a comprehensive list

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Control Analysis

Purpose

- To analyze the controls that have been implemented, or planned for implementation to minimize or eliminate the likelihood of a threat exercising a system vulnerability

Risk Assessment – Control Analysis

Control Methods

- **Technical** controls are safeguards incorporated into computer hardware, software or firmware
- **Non-technical** controls are administrative and physical controls
  - Security policies
  - Standard operating procedures
  - Physical security
  - Personnel security
  - Environmental security

Risk Assessment – Control Analysis

Control Categories

- Preventive controls inhibit attempts to violate security policy
  - Control enforcement
  - Encryption
  - Authentication
- Detective controls warn of violations or attempted violations of security policy
  - Audit trails
  - Intrusion detection methods
  - Checksums

Risk Assessment – Control Analysis

Summary

- The output of step 4 is a list of current or planned controls used by the IT system to mitigate the likelihood that a vulnerability will be exercised and reduce the impact of such an adverse event

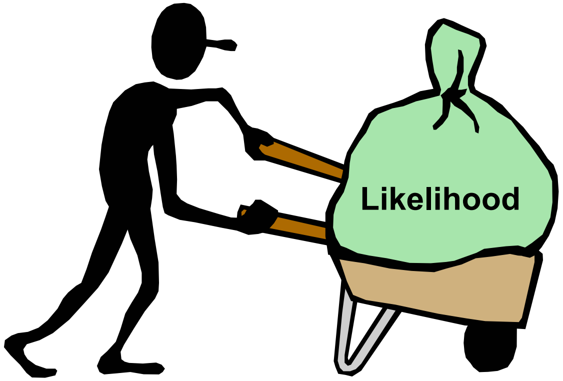
Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Likelihood Determination

Purpose

- To derive an overall likelihood rating of probability that a potential vulnerability may be exercised considering:
  - Threat-source motivation and capability
  - Nature of vulnerability
  - Existence and effectiveness of current controls



Risk Assessment – Likelihood Determination

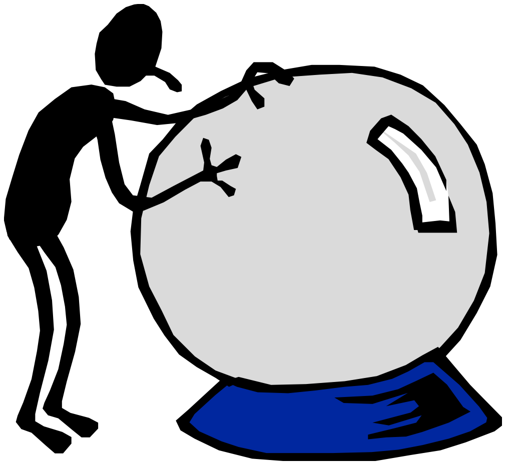
Likelihood Rating

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable and/or controls to prevent the vulnerability are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent or significantly impede the vulnerability from being exercised

Risk Assessment – Likelihood Determination

Summary

- The output of Step 5 is a likelihood rating, in terms of *high*, *medium*, or *low*, that each identified vulnerability will be exercised by its associated threat



Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Impact Analysis

Purpose

- To determine the adverse impact resulting from a successful threat exercise of a vulnerability
- Information needed for analysis
  - Organization mission
  - System and data criticality
  - System and data sensitivity

Risk Assessment – Impact Analysis

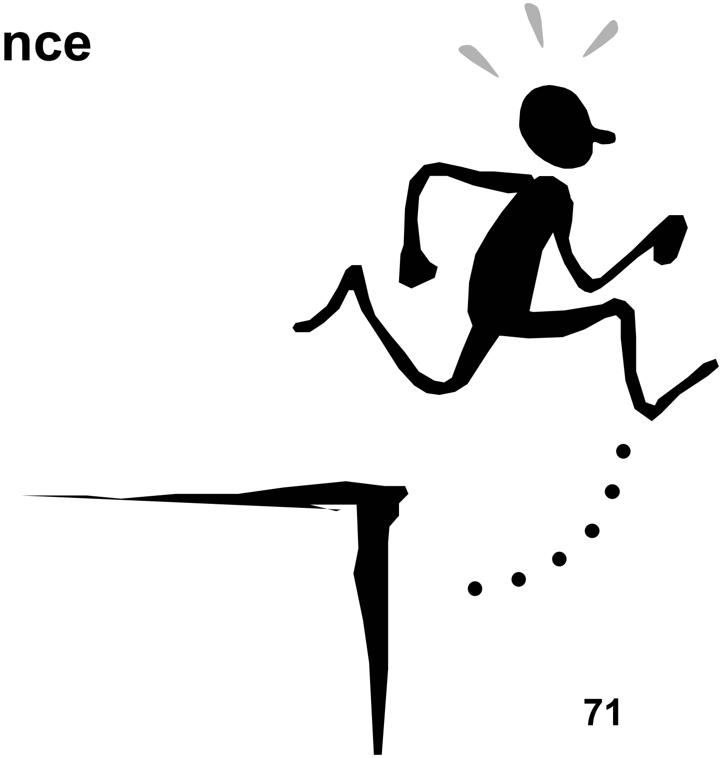
Outcome of a Security Event

- **Loss of Integrity** – Unauthorized changes are made to data or IT system (intentional or accidental)
- **Loss of Availability** – May result in loss of productive time impeding the end users’ performance of functions supporting the organization’s mission
- **Loss of Confidentiality** – Unauthorized disclosure of information may range from jeopardizing of national security to the disclosure of protected health information

Risk Assessment – Impact Analysis

Impact of the Outcome

- Consider the impact to the organization of an unauthorized disclosure, unauthorized modification, unauthorized destruction or denial of access in all of the following areas:
  - Reputation and customer confidence
  - Life and health of customers
  - Productivity
  - Fines and legal penalties
  - Financial
  - Readiness



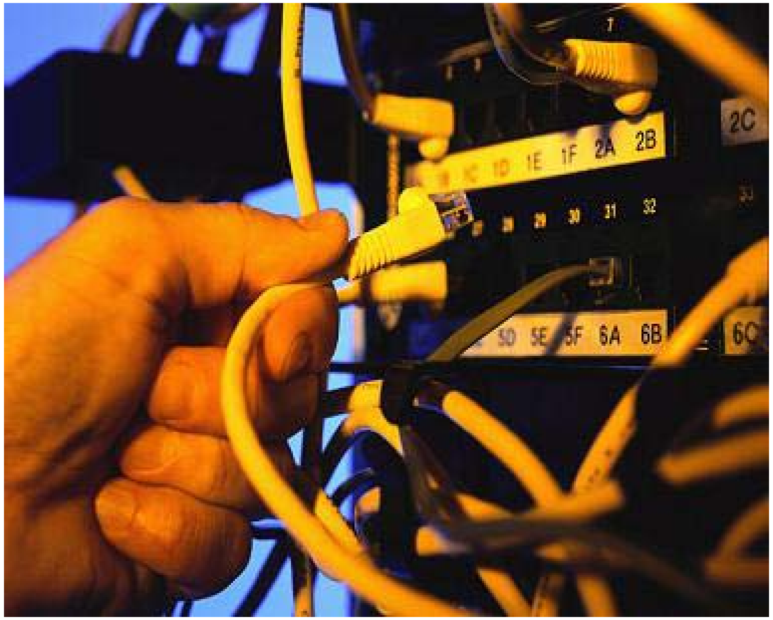
Impacting Business (1 of 3)

- **Tangible Losses - Confidentiality Breach**
  - Loss of intellectual property
  - Consulting/legal fees
  - Public relations
  - Cost of business

Risk Assessment – Impact Analysis

Impacting Business (2 of 3)

- **Tangible Losses - Integrity Breach**
  - Data Recovery and Reconstitution Cost
  - Consulting/Legal Fees
  - Loss of User Productivity



Risk Assessment – Impact Analysis

Impacting Business (3 of 3)

- **Tangible Losses – Loss of Availability**
  - Decrease in user productivity
  - Loss of business revenue
  - Disaster recovery costs

Risk Assessment – Impact Analysis

Output

- The output of Step 6 is a magnitude of impact rating, in terms of *high*, *medium*, or *low,* for each threat-vulnerability pair
  - The magnitude of impact rating which can be used in a cost-benefit analysis of recommended controls

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Risk Determination

Purpose

- To assess the level of risk to the IT systems and the information of the organization
- The determination of risk for a particular threat-vulnerability can be expressed as a function of
  - The likelihood of a given threat source's attempting of exercise a given vulnerability
  - The magnitude of the impact should the threat-source exercise the vulnerability
  - The adequacy of planned or existing security controls for reducing or eliminating risk

Risk Assessment – Risk Determination

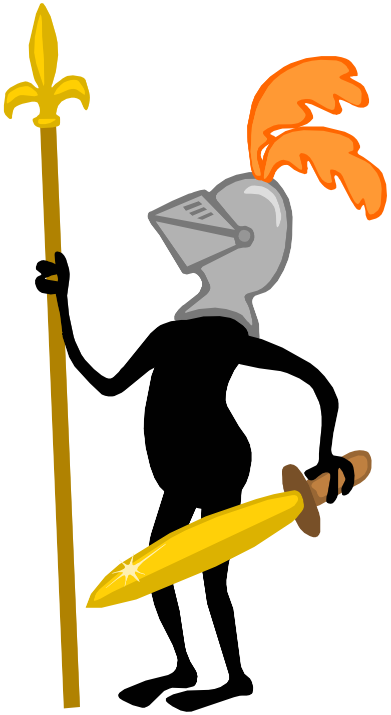
Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be in place as soon as possible
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk

Risk Assessment – Risk Determination

Output

- The output of step 7 is a risk-level rating for each threat-vulnerability pair
- The rating indicates what actions should be taken to mitigate the risk



Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Control Recommendations

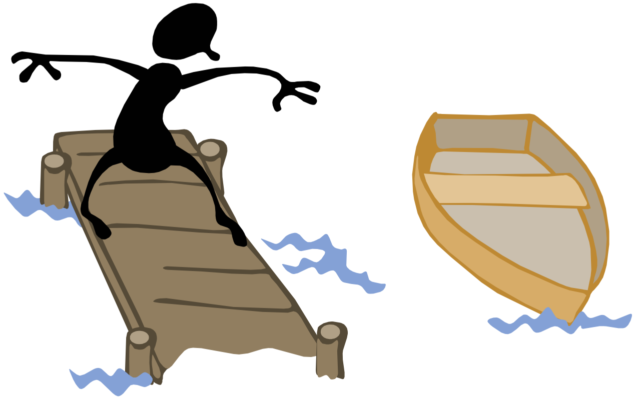
Purpose

- To reduce the level of risk to the IT system and its data to an acceptable level
- Factors in recommending controls and alternative solutions
  - Effectiveness of recommended options
  - Legislation and regulations
  - Organizational policy
  - Operational impact
  - Safety and reliability
  - Cost

Risk Assessment – Control Recommendations

Remember….

- Some solutions may provide multiple services
- Placement of the service is critical
- Need balance between what's appropriate and cost effective



Risk Assessment – Control Recommendations

Output

- The output of Step 8 is a recommendation of control(s) and alternative solutions to mitigate risk

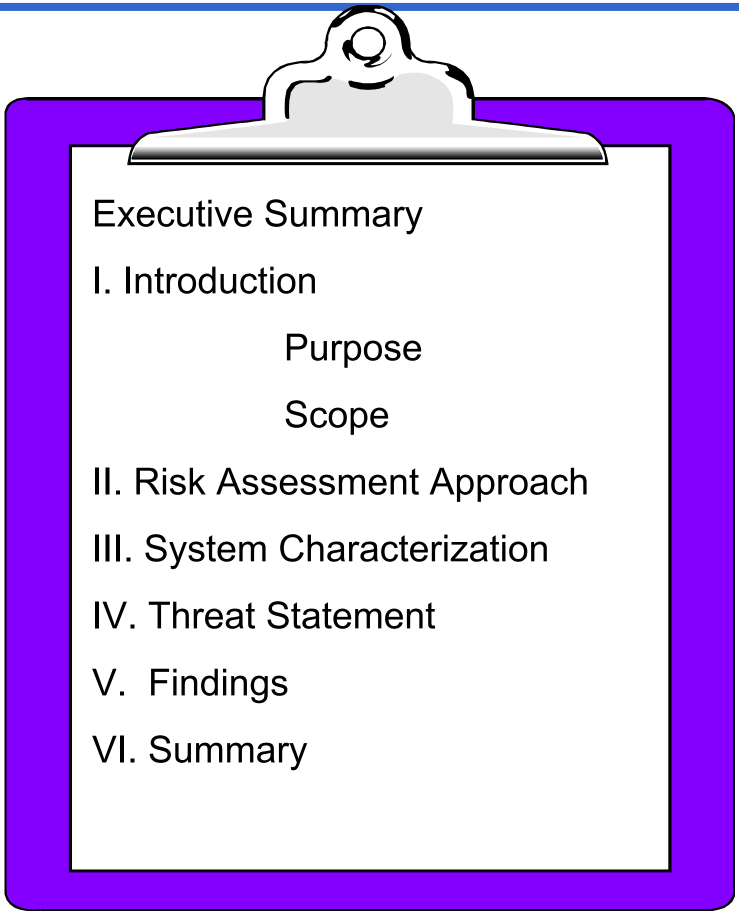
Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Assessment – Results Documentation

Purpose

- The results of the risk assessment should be documented in a report



Executive Summary

I. Introduction

Purpose

Scope

II. Risk Assessment Approach

III. System Characterization

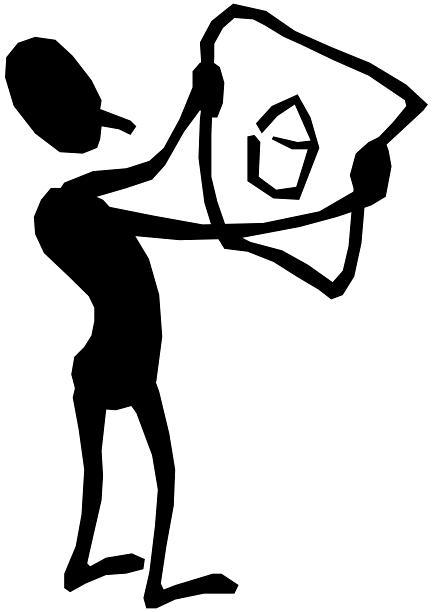
IV. Threat Statement

V. Findings

VI. Summary

Risk Assessment – Results Documentation

Report Contents



- The risk assessment report should be of sufficient detail to allow the organization’s management to make informed decisions on appropriate actions in response to the risks identified

Risk Assessment – Results Documentation

Risk Assessment Report Outline

- Executive Summary

I. Introduction

II. Risk Assessment Approach

III. System Characterization

IV. Threat Statement

V. Risk Assessment Results

VI. Summary

Risk Assessment Report

Introduction

- Purpose
- Scope
- Describe
  - System Components
  - Elements
  - Users
  - Site locations
  - Other details as necessary

Risk Assessment Report

Risk Assessment Approach

- Describe approach used
  - Risk Assessment Team members
  - Techniques used to gather information (use of tools, questionnaires, etc)
  - Development and description of risk scale (3x3, 4x4, or 5x5 risk level matrix)

Risk Assessment Report

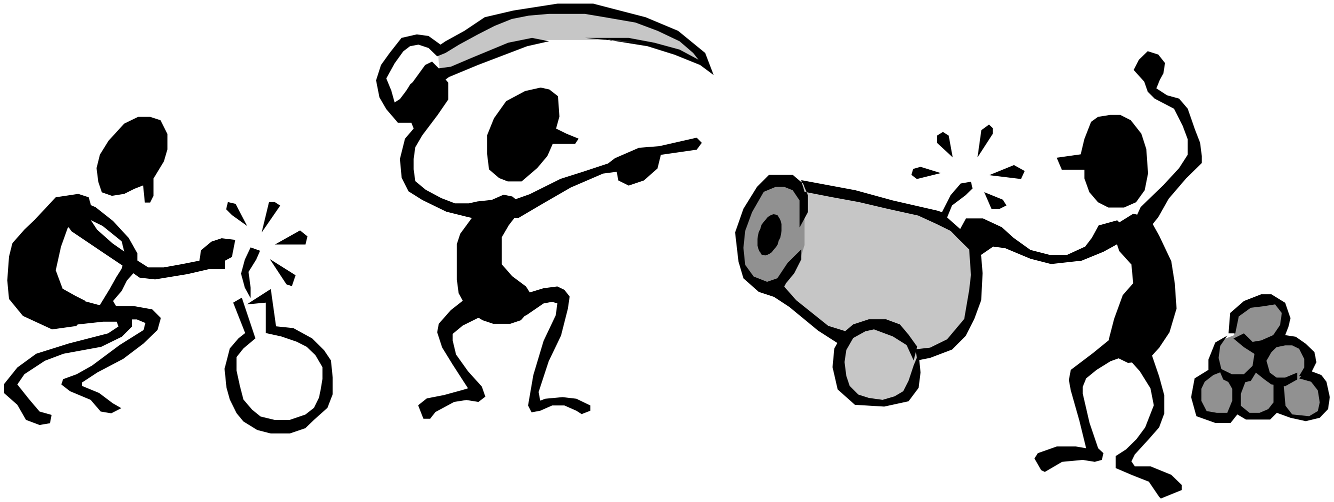
System Characterization

- Describe the system
  - Hardware (server, router, switch)
  - Software (application, operating system, protocol)
  - System Interfaces (communication link)
  - Data
  - Users
- Provide connectivity diagram or system input and output flowchart

Risk Assessment Report

Threat Statement

- Compile potential threat sources
- List associated threat actions



Risk Assessment Report

Risk Assessment Results

- List observations (vulnerability/threat pairs)
- Observations contain:
  - Observation number and brief description
  - Discussion of threat-source and vulnerability pair
  - Identification of existing mitigation security controls
  - Likelihood discussion and evaluation
  - Impact analysis discussion and evaluation
  - Risk rating
  - Recommended controls or alternative options

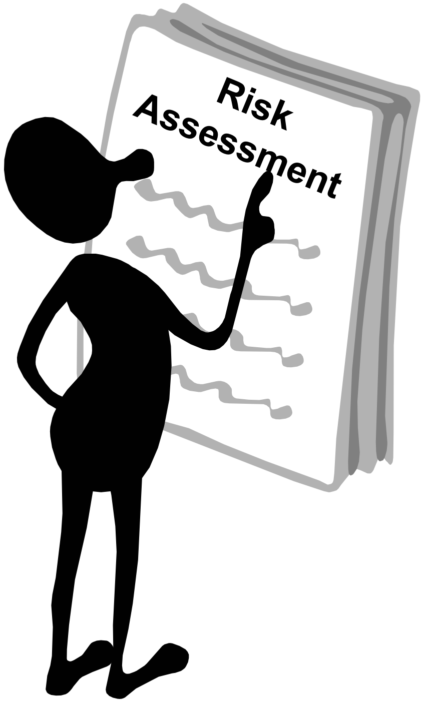
Risk Assessment Report

Summary

- Total number of observations
- Summarize
  - Observations
  - Associated risk levels
  - Recommendations
  - Any comments
- Organize into a table to facilitate implementation

Risk Assessment – Results Documentation

Output

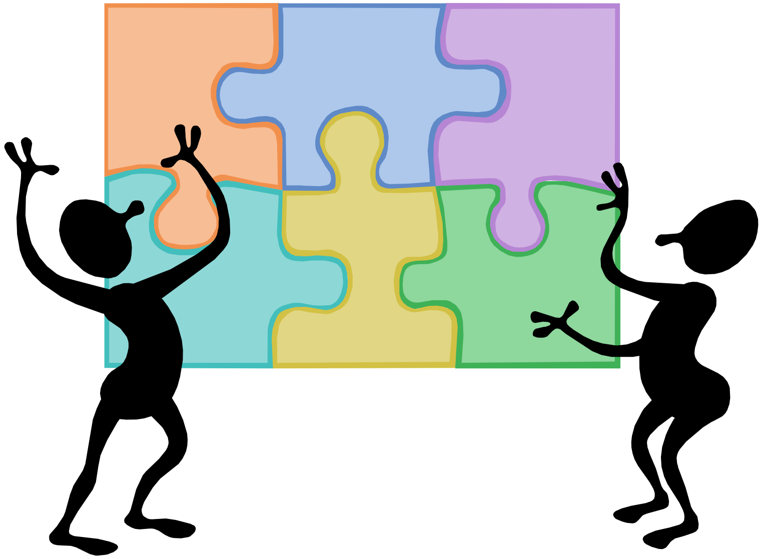


- The output of Step 9 is the completed risk assessment report

Risk Assessment

The Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact analysis
7. Risk Determination
8. Control Recommendation
9. Results Documentation



Risk Assessment

What do you think?

- Three kinds of threats are: natural, manmade, and ____________
- Adverse impacts of a security event are loss of _________ , availability, or confidentiality
- The ____________________ should include enough detail to allow managers to make informed decisions on appropriate actions in response to identified risks

Summary

- You should now be able to:
  - Describe risk assessment
  - Define threats
  - List and describe the nine-steps of the risk assessment methodology

Risk Mitigation

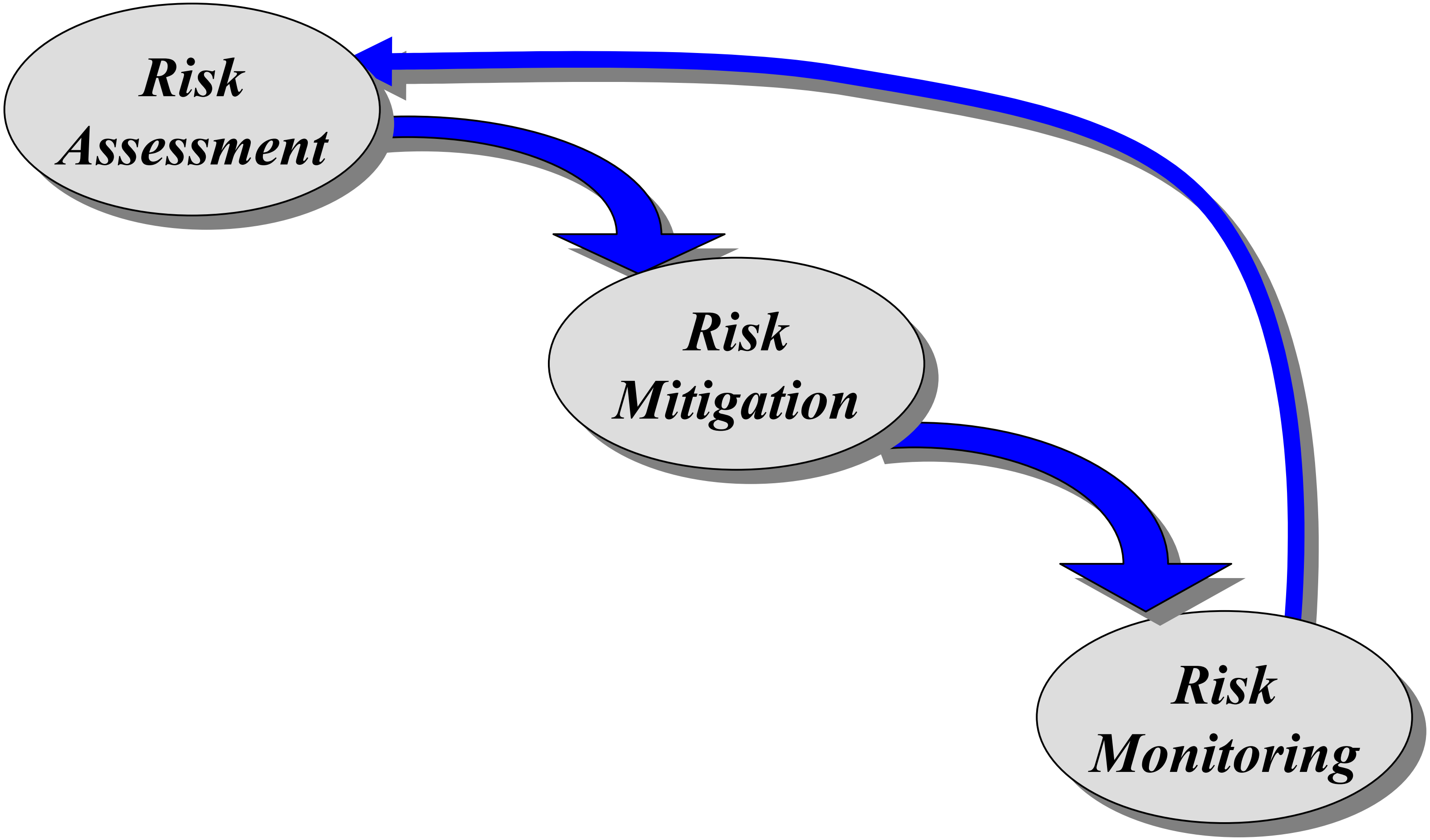
Risk Mitigation

Objectives

- After completing this module, you should be able to:
  - Describe the components of risk mitigation
  - List and describe who is involved in the risk mitigation process
  - Describe risk mitigation options

Risk Mitigation

Risk Management Process



What is Risk Mitigation?

- The process of identifying areas of risk that are unacceptable; and estimating countermeasures, costs and resources to be implemented as a measure to reduce the level of risk

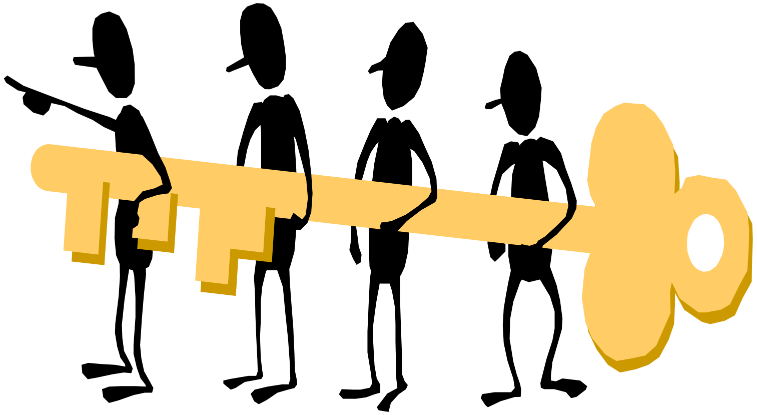
Purpose

- To enable management to make informed decisions regarding countermeasure analysis against known risk to a system(s)

Risk Mitigation

Who is involved?

- Risk determinations are not made in isolation. Decisions must include Management and Business Owners
- Recommended Staff involvement:
  - Executive Council
  - Clinical Representative
  - Business Process Owners
  - Comptroller
  - Billing Office
  - Personnel Office/Human Resources
  - CIO
  - ISSO
  - Patient Administration/Medical Records



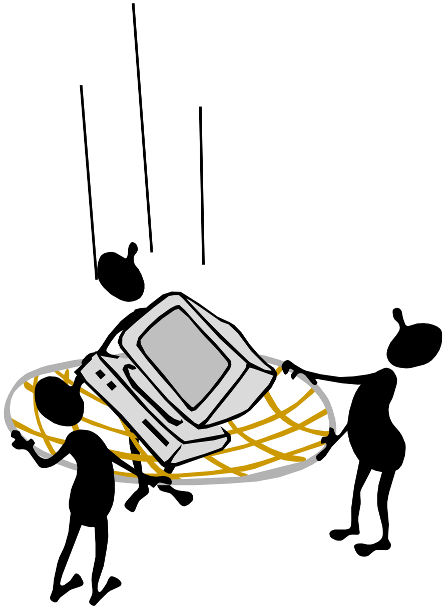
Risk Mitigation

Ultimate Responsibility

- It is the decision of the Commander (DAA) of the facility to assume a level of risk
- It is a business decision and should align with strategic and capital planning initiatives

Risk Mitigation Decisions

- Elimination of all risk is realistically impossible
- Management generally uses the most cost-effective approach and implements the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization’s resources and mission



Risk Mitigation Options (1 of 2)

- **Options** for risk mitigation depend on an organization's goals and mission
  - **Risk assumption** = accept potential risk and continue operation or implement controls to lower risk to an acceptable level
  - **Risk avoidance** = avoid risk by eliminating the cause and/or consequence
  - **Risk limitation** = limit risk by implementing controls that minimize adverse impact

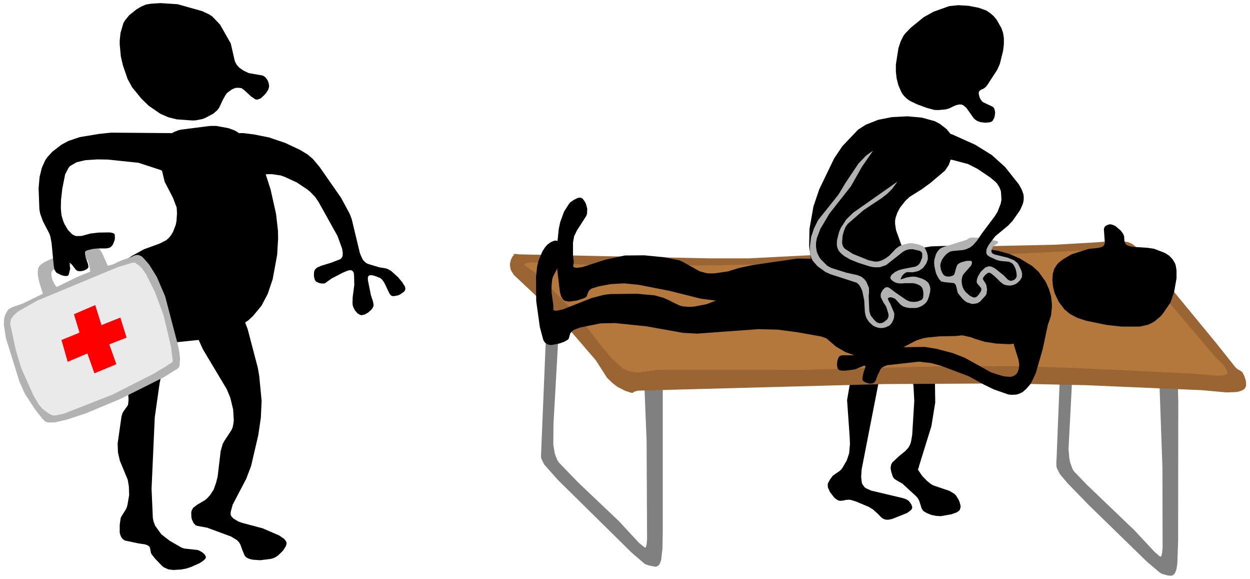
Risk Mitigation Options (2 of 2)

- **Options** continued
  - **Risk planning** = developing a risk mitigation plan that prioritizes, implements, and maintains controls
  - **Research and acknowledgement** = acknowledge vulnerability and researching corrective actions
  - **Risk transfer** = using other options, such as insurance, to compensate for the loss

Risk Mitigation

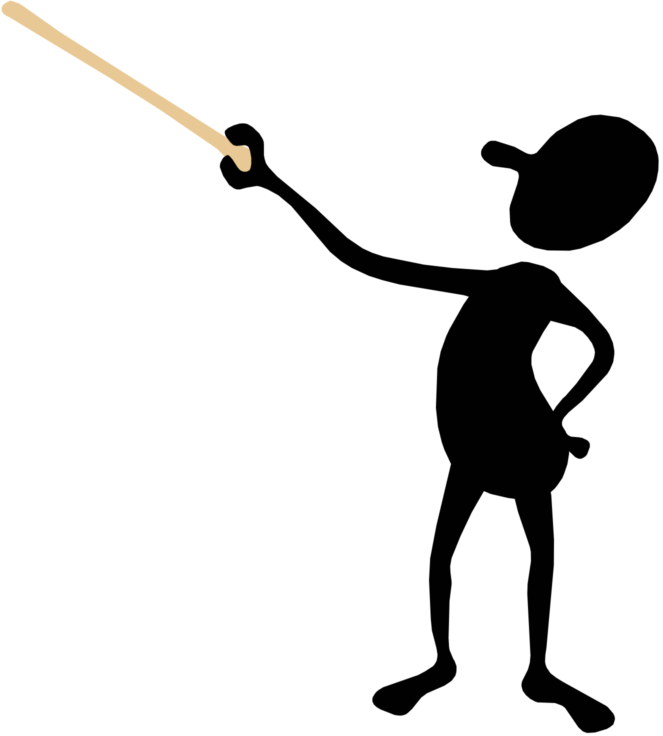
Considerations

- To make the best determination for Risk Mitigations, consider outcomes and impact



Risk Mitigation Steps

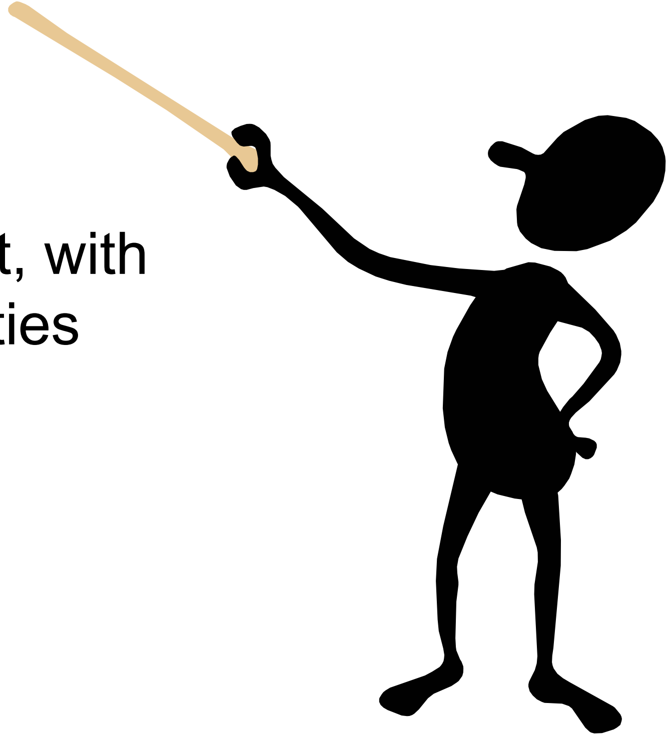
- Step 1. Determine approach to handle the risk
- Step 2. Develop risk mitigation plan
- Step 3. Implement and Document



Risk Mitigation Steps

Step 1 – Determine Approach

- Determine approach to handle the risk
  - What are the options for mitigating that risk?
- Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities



Step 1 - Determine Approach

Activities

A. Prioritize risks and identify mitigation options

B. Evaluate recommended mitigation options

C. Conduct cost-benefit analysis

Step 1 - Determine Approach

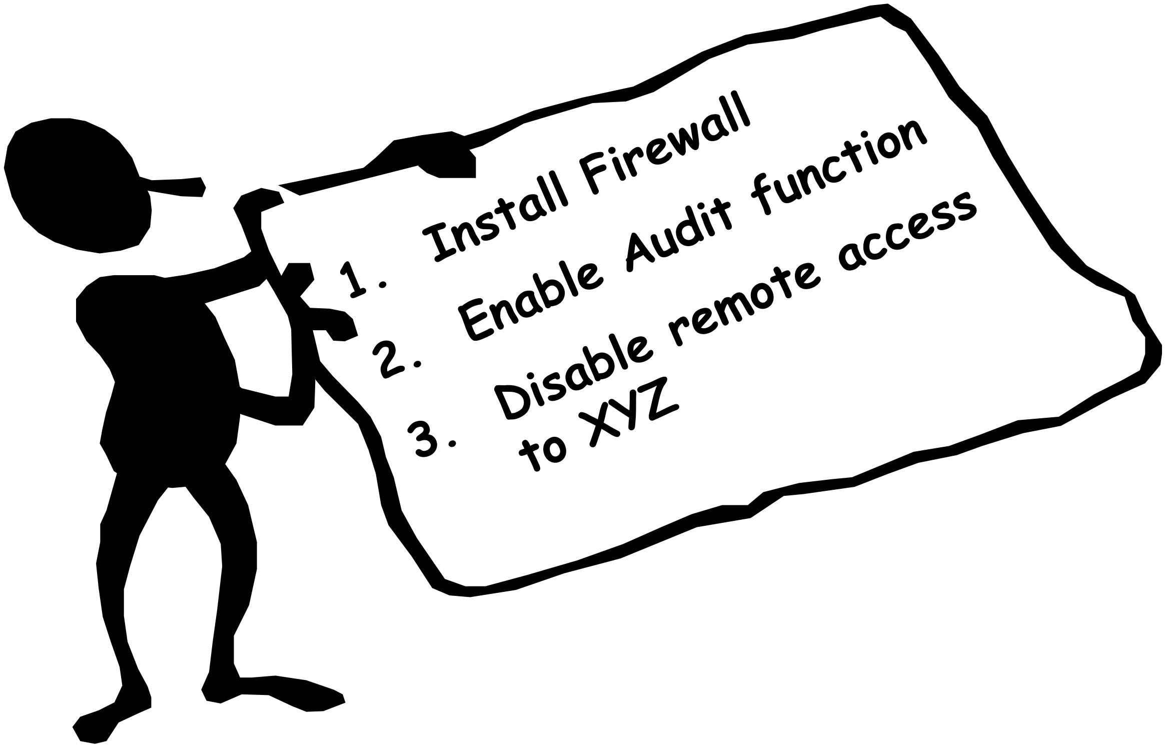
Activity A – Prioritize Risks

- From Risk Assessment Report, review the prioritized risks and mitigation options
  - Risk rankings of High are top priority
  - High priority items require immediate actions to protect organization’s mission and interests

Step 1 - Determine Approach

Activity A – Prioritize Risks

- Examples of Options:
  - Actions ranking from High to Low



Step 1 - Determine Approach

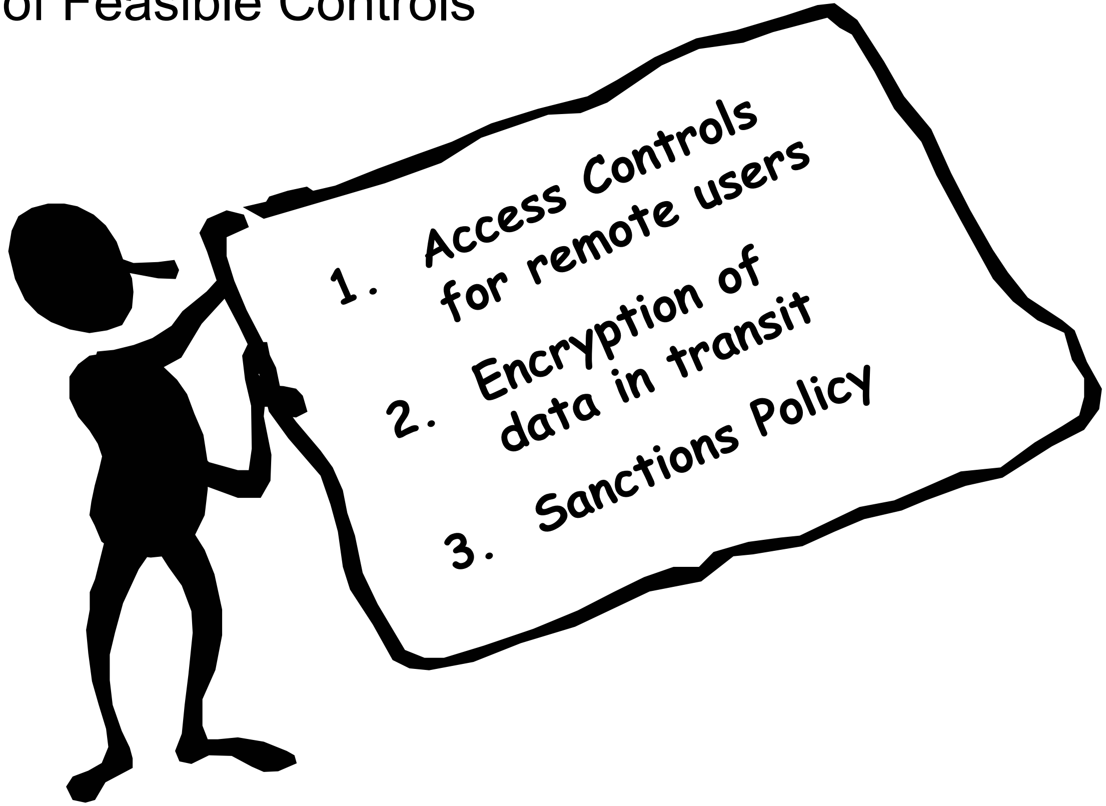
Activity B – Evaluate Recommended Control Options

- For each option, evaluate
  - Feasibility
    - Compatibility
    - User Acceptance
  - Effectiveness
    - Degree of protection
    - Level of risk mitigation

Step 1 - Determine Approach

Activity B – Evaluate Recommended Control Options

- Outcome:
  - List of Feasible Controls


1. Access Controls for remote users
2. Encryption of data in transit
3. Sanctions Policy

Step 1 - Determine Approach

Activity C – Conduct Cost-Benefit Analysis

- Chose methodology: qualitative or quantitative
- Is the cost of implementing the controls justified by the reduction of the level of risk?
- Option must support the mission of the organization

Step 1 - Determine Approach

Activity C – Conduct Cost-Benefit Analysis

- Impact of implementing new or enhanced controls
- Impact of NOT implementing new or enhanced controls
- Estimating cost
  - Hardware and software
  - Reduced operational effectiveness if system performance is reduced for increased security
  - Implementing additional policies and procedures
  - Hiring additional staff
  - Training
  - Maintenance
- Assess the implementation costs and benefits against the system and data criticality

Step 1 - Determine Approach

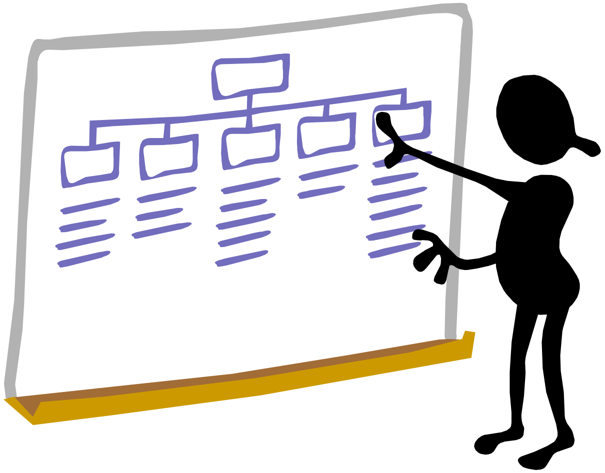
Activity C – Conduct Cost-Benefit Analysis

- Outcome:
  - Cost benefit analysis describing the cost and benefits of implementing or not implementing the controls
- Remember: Risk in a healthcare environment is unique with special factors
  - Life
  - Limb
  - Suffering
  - Safety

Risk Mitigation Steps

Step 2 – Develop Risk Mitigation Plan

- Develop risk mitigation plan
  - What to document on the plan?
- The strategy to mitigate risks identified. Should include a plan of action with specific tasks, responsible personnel, and dates for completion

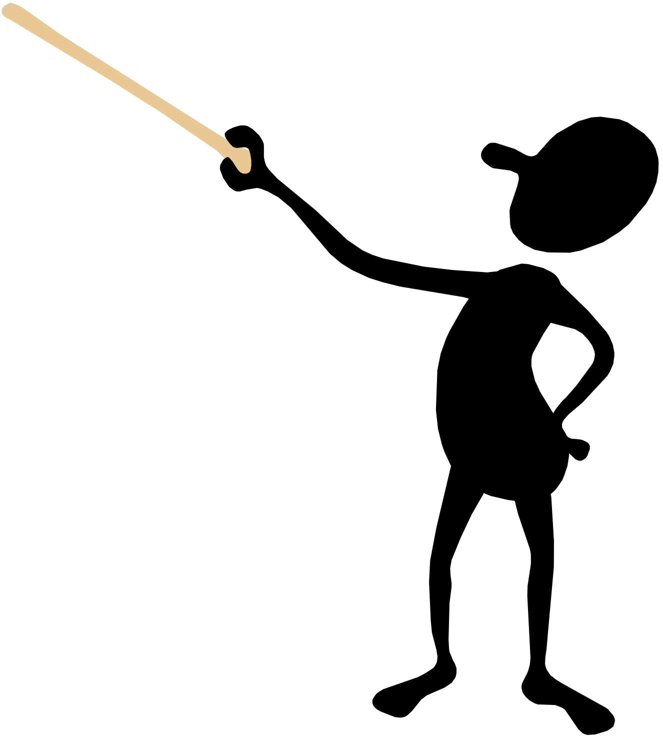


Step 2 – Develop Plan
Activities

A. Select Control

B. Assign Responsibility

C. Develop an Implementation Plan



Step 2 – Develop Plan

Activity A – Select Controls

- Select controls based on the cost benefit analysis and the control evaluation
- Combine controls from:
  - Administrative
  - Physical
  - Technical
- Controls ensure security for the IT systems, the data, and the organization

Step 2 – Develop Plan

Activity A – Select Controls

- Outcome:
  - List of Selected Controls

1. Sanctions Policy
2. Access Controls for remote users

Step 2 – Develop Plan

Activity B – Assign Responsibility

- Identify appropriate personnel
  - Internal personnel or external contracting staff
  - Appropriate expertise and skill-sets
- Assign responsibility

Step 2 – Develop Plan

Activity B – Assign Responsibility

- Outcome
  - List of responsible persons

1. CIO
2. Personnel Officer
3. Security Officer

Step 2 – Develop Plan

Activity C – Develop an Action Plan

- Action Plan
  - Prioritizes the implementation actions
  - Projects start and completion dates
  - Aids and expedites the risk mitigation process

Step 2 – Develop Plan

Activity C – Develop an Action Plan

- Action Plan contains:
  - Prioritized Actions
  - Selected controls
  - Required resources
  - Lists of responsible teams and staff
  - Start date for implementation
  - Target complementation date
  - Action plan maintenance requirements

Risk Mitigation Steps

Step 3 – Implement and Document

A. Implement controls that mitigate risk by:

- Following the action plan
- Monitoring progress
- Communicating status

B. Update system security plan and related security documentation

Step 3 – Implement and Document

Activity A - Implement Selected Controls

- Outcome:
  - Reduction in risk
  - Compliance with documentation requirements

- Remember: Residual Risk that is not eliminated by the implemented controls must be accepted by DAA or senior management

Summary: Risk Mitigation Steps

- Step 1. Determine approach to handle the risk
- Step 2. Develop risk mitigation plan
- Step 3. Implement and Document

Risk Monitoring

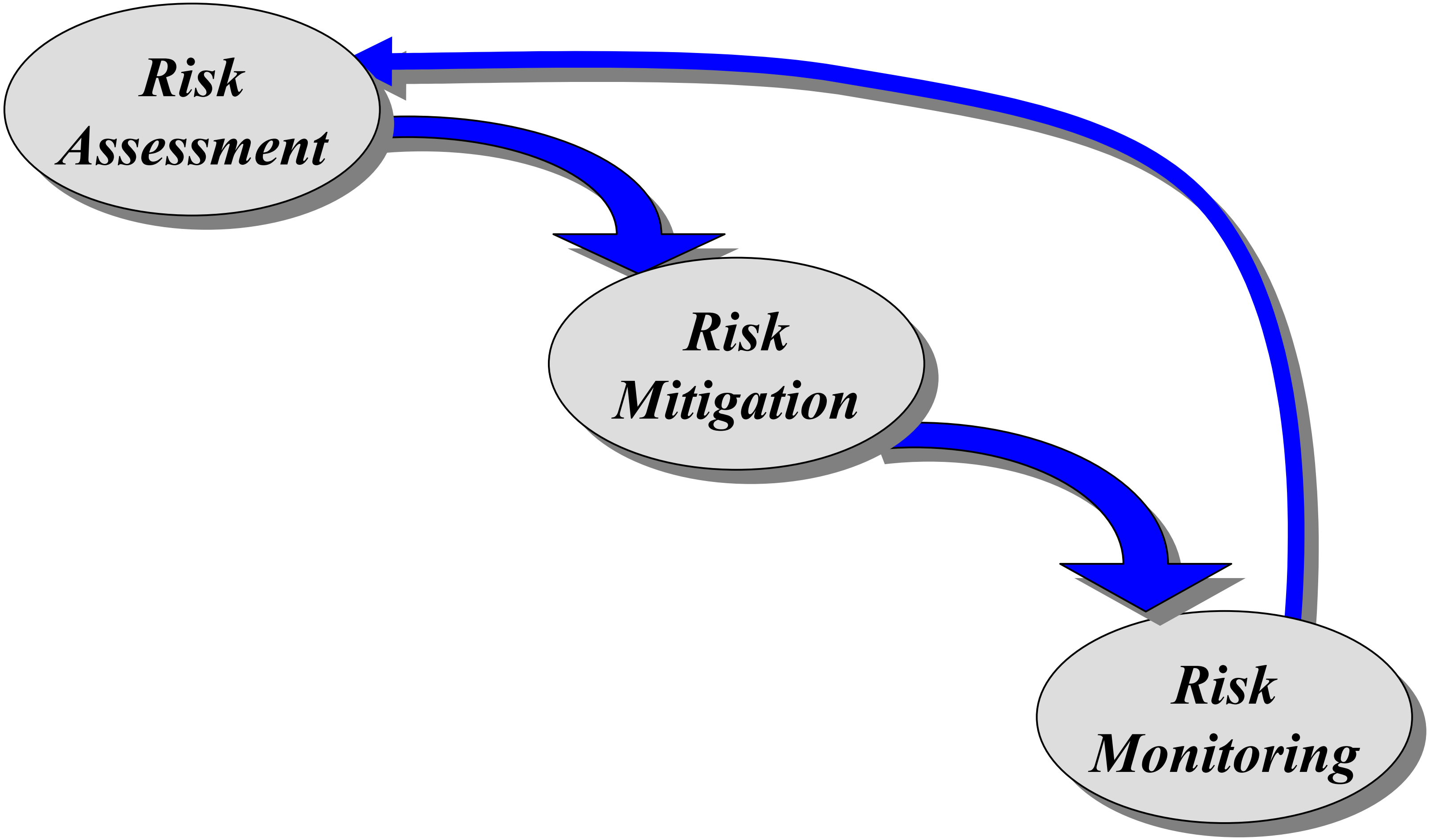
Risk Monitoring

Objectives

- After completing this module, you should be able to:
  - Identify where risk monitoring fits in the Risk Management process
  - Describe the frequency of risk monitoring
  - Identify factors that will change the risk status of your systems

Risk Monitoring

Risk Management Process



Continual Monitoring

- Key for implementing a successful risk management program
- Necessary to keep your organization at the risk level that was deemed acceptable

Risk Monitoring

Activities

- Utilize automated tools for vulnerability scanning
- Subscribe to vulnerability list services
- Check frequently for
  - New anti-virus updates
  - Critical updates to operating systems
  - Patches

Risk Monitoring

Review Schedule

- Establish the frequency of reviews of audit and system activity logs, taking into account the following factors :
  - Sensitivity of the information (EPHI)
  - Size of the facility
  - Complexity of the organization

Risk Monitoring

Review Schedule

- Repeat evaluations when significant changes to the security environment are made
- Examples of changes:
  - Network expanded
  - Components changed
  - Software Applications replaced
  - Personnel rotated
  - New vulnerabilities and threats emerged

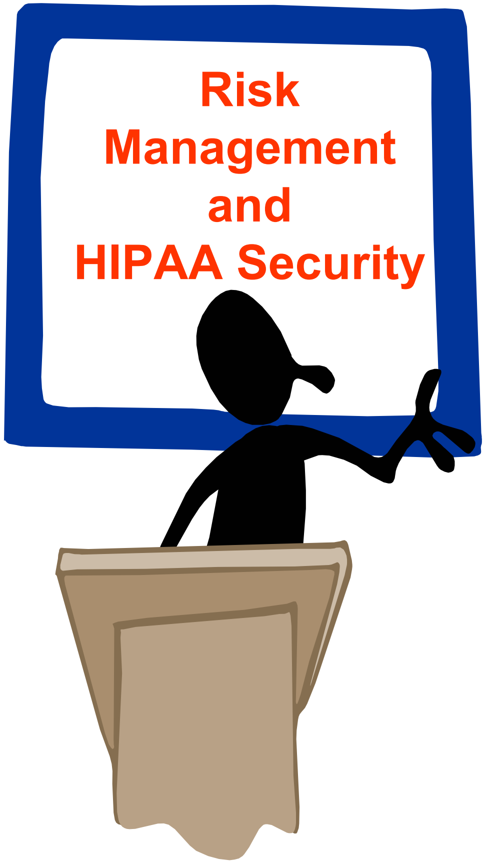
Risk Monitoring

Summary

- You should now be able to:
  - Identify where risk monitoring fits in the Risk Management process
  - Describe the frequency of risk monitoring
  - Identify factors that will change the risk status of your systems

Risk Management and HIPAA Security

Objectives



- After completing this module, you should be able to:
  - List the elements of risk management in the HIPAA Security Rule
  - Describe how the risk management process supports HIPAA security compliance
  - Identify common mistakes that will impede compliance

Information Security….

- Remember our definition of Information Security?

Information security is achieved through an integrated system of policies, procedures, products, and people that identify, control, and protect information from unauthorized disclosure and by an information protection strategy that is authorized by management and integral to good business practice.

….and the HIPAA Security Rule

- One of the primary components of a sound information security program is risk management
  - Called the "Security Management Process" in the HIPAA Security Rule
  - Standard:

A covered entity must implement policies and procedures to prevent, detect, contain and correct security violations

Security Management Process

- First administrative safeguard
- Implementation Specifications include:
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review

Security Management Process vs Risk Management

Correlation

HIPAA Security Management Process	Risk Management Process
• Risk Analysis	Risk Assessment
• Risk Management	Risk Mitigation
• Sanction Policy	??
• Information System Activity Review	Risk Monitoring

Security Management Process vs Risk Management

Alignment (1 of 3)

- Risk Analysis = Risk Assessment
  - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI
  - These activities result in the same outcome as the nine steps for risk assessment
- Key difference – Risk analysis from the HIPAA perspective requires an assessment for EPHI only

Security Management Process vs Risk Management Alignment (2 of 3)

- Risk Management (HIPAA Implementation Standard) and risk mitigation are both implementation phases
  - Require implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to prevent, detect, contain and correct security violations
  - Identifying areas of risk that are unacceptable
  - Estimating countermeasures, costs and resources

Security Management Process vs Risk Management Alignment (3 of 3)

- Information System Activity Review = Risk Monitoring
  - Both require the implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking
  - Necessary to keep your organization at the risk level that was deemed acceptable
- Key difference – HIPAA requirement for review pertains to information system activity only

Security Management Process vs Risk Management

What’s Different?

- Risk management process has no specific component for sanctions

- Security Management Process
  - Requires a sanction policy that enables organizations to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of your organization

Security Management Process vs Risk Management

Sanction Policy

- Why is it necessary?
  - Because the greatest risk is always from inside the organization
  - Administrative control to mitigate the risk from personnel
  - Lowers and maintains risk at an acceptable level

Conclusion

Risk Management

+ Sanctions Policy

Security Management Process

Security Management Process vs Risk Management

So What?

- Now that we understand risk management in the context of HIPAA, what are the issues that we need to be aware of?

An Assessment of HIPAA
Security Preparedness:
Most Health Care Organizations
Remain Noncompliant
A report published by URAC in April 2004

- Essence of the findings is that medical organizations did not apply the comprehensive concepts of risk management to the HIPAA requirements

Security Management Process vs Risk Management

Report Findings

- Results show the top 3 mistakes are all risk management activities with significant impacts
  - Rule states that “Risk management activities are the foundations upon which a security program are built.”
  - Therefore, a faulty foundation leads to a weak program
- Top three mistakes relate to:
  - Risk Analysis efforts
  - Risk Management strategies
  - Information System Activity Review

Risk Management and HIPAA Security

Top Three Common Mistakes

- Risk Analysis efforts
- Risk Management strategies
- Information System Activity Review

Top Three Common Mistakes

Risk Analysis Efforts (1 of 3)

- Risk analysis efforts were incomplete and inappropriately scoped

- Key factors for a comprehensive risk analysis that were lacking:
  - Understanding of the EPHI possessed
    - Uses of that EPHI
  - Likelihood that EPHI may be compromised
    - Impact of a compromise

Top Three Common Mistakes

Risk Analysis Efforts (2 of 3)

- Risk analysis efforts did not result in a formal identification of the organization’s:
  - Risk tolerance
  - Residual risk
  - Prioritization of subsequent risk reduction activities
- Documentation was not comprehensive enough to serve as the primary piece of evidence for:
  - Review by CMS in response to any complaints
  - Documenting due diligence and rationale for reasonable and appropriate controls

Top Three Common Mistakes

Risk Analysis Efforts (3 of 3)

- Organizations failed to conduct comprehensive evaluations beyond a typical vulnerability assessment

– Vulnerability assessment
  - Identification of the potential issues that could be exploited

– Risk Analysis is a systemic and detailed:
  - Identification of likely threats
  - Vulnerabilities
  - Likely impacts
  - Recommended security controls

Risk Management and HIPAA Security

Top Three Common Mistakes

- Risk Analysis efforts
- Risk Management strategies
- Information System Activity Review

Top Three Common Mistakes

Risk Management Strategies (1 of 5)

Risk management strategies were inconsistent and poorly executed

- Faulty data for risk management decisions
  - Based on non-comprehensive results of the risk analysis
- Resources were not allocated appropriately
  - Necessary to gain the highest level of risk reduction in alignment with the organization’s risk tolerance

Top Three Common Mistakes

Risk Management Strategies (2 of 5)

- Assumption of risk
  - Decisions are made by IT professionals without the guidance and support from business operations
  - Failure to utilize combinations of administrative, physical and technological controls
    - Rely too heavily upon technical controls

Top Three Common Mistakes

Risk Management Strategies (3 of 5)

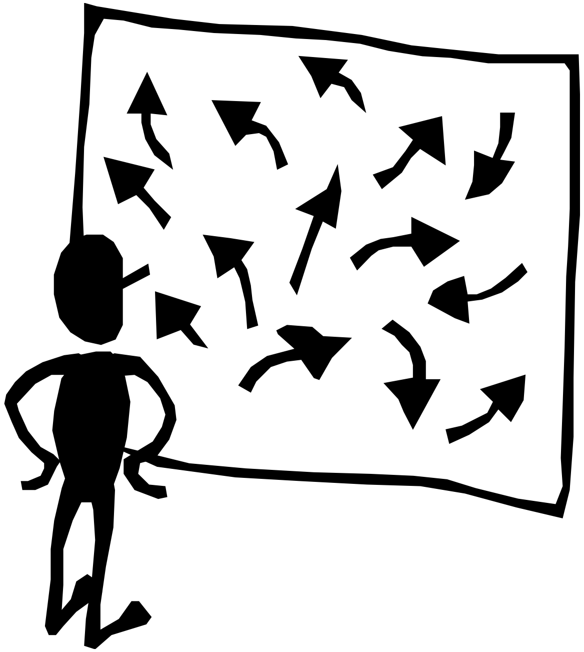
- Organizations are failing to plan for the effective:
  - Deployment
  - Maintenance
  - Upgrade

….of selected Security Controls

Top Three Common Mistakes

Risk Management Strategies (4 of 5)

- Serious weaknesses with Policy and Procedure:
  - Documentation
  - Management
  - Implementation



Top Three Common Mistakes

Risk Management Strategies (5 of 5)

- Policy and practice inconsistencies
  - Ignored because of perceived management indifference
  - Impossible to execute because of inadequate resources and tools
  - Verification of implementation did not occur at regular intervals

Risk Management and HIPAA Security

Top Three Common Mistakes

- Risk Analysis efforts
- Risk Management strategies
- Information System Activity Review

Top Three Common Mistakes

Information System Activity Review (1 of 5)

- Information system activity review was limited and faulty
  - Sites collected data from audit logs but did not review or analyze
  - Reviewed limited records (e.g. Access logs) only when a security incident occurred

Top Three Common Mistakes

Information System Activity Review (2 of 5)

- Information system activity reviews failed to:
  - Provide an accurate history of system activity in the event of a security breach
  - Allows organizations to:
    - Track system usage (such as use and disclosure patterns of PHI)
    - Reconstruct, review and examine events
    - Detect and verify unauthorized users and processes

Top Three Common Mistakes

Information System Activity Review (3 of 5)

- Organizations did not have a plan for the scope and frequency of reviews
- Plan elements that were lacking:
  - Determination of data elements that must be captured to detect a security breach
    - Focus must be on the use and disclosure of EPHI

Top Three Common Mistakes

Information System Activity Review (4 of 5)

- Plan elements that were lacking (cont):
  - Determination of frequency in which data will be reviewed and analyzed
    - Audits may be daily, weekly, monthly and quarterly with increasing level of data points

Top Three Common Mistakes

Information System Activity Review (5 of 5)

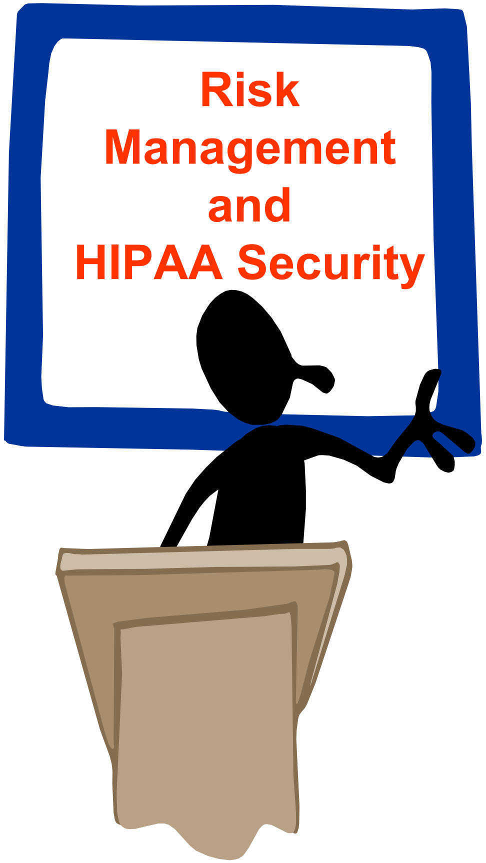
- Did not employ multiple analysis methods:
  - Not possible to just “eye-ball” data to identify any interesting events
  - Requires assistance of activity review tools and additional technologies
    - Able to analyze trends
    - Retroactively review data post-incident

Closure

- Keep these findings in mind and avoid making these common mistakes
  - Risk analysis efforts need to be comprehensive and appropriately scoped
  - Risk management strategies depend on the results of the risk analysis and must be:
    - Consistently executed
    - Supported by management
    - Properly resourced
  - Information system activity reviews must be planned and have a defined purpose

Risk Management and HIPAA Security

Summary



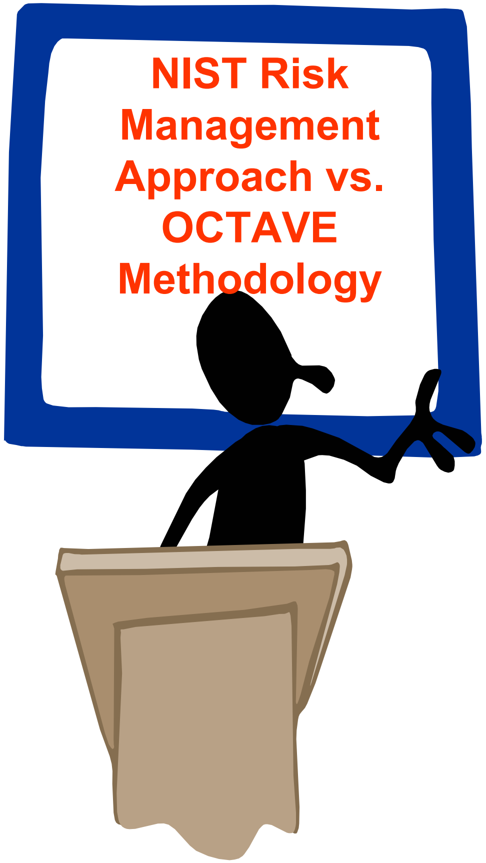
- You should now be able to:
  - List the elements of Risk Management in the HIPAA Security Rule
  - Describe how the Risk Management process supports HIPAA Security Compliance
  - Identify common mistakes that will impede compliance

OCTAVE Methodology vs. NIST Risk Management Approach

(Comparative Analysis)

OCTAVE Methodology vs. NIST Risk Management Approach

Objectives



- After completing this module, you should be able to:
  - Locate the report on *OCTAVE-Best Practices Comparative Analysis*
  - Describe the general phases of the OCTAVE methodology
  - Describe the general steps of the NIST approach
  - Describe how OCTAVE differs from the NIST risk assessment approach
  - Identify common elements between the two methodologies

OCTAVE Methodology vs. NIST Risk Management Approach

Report

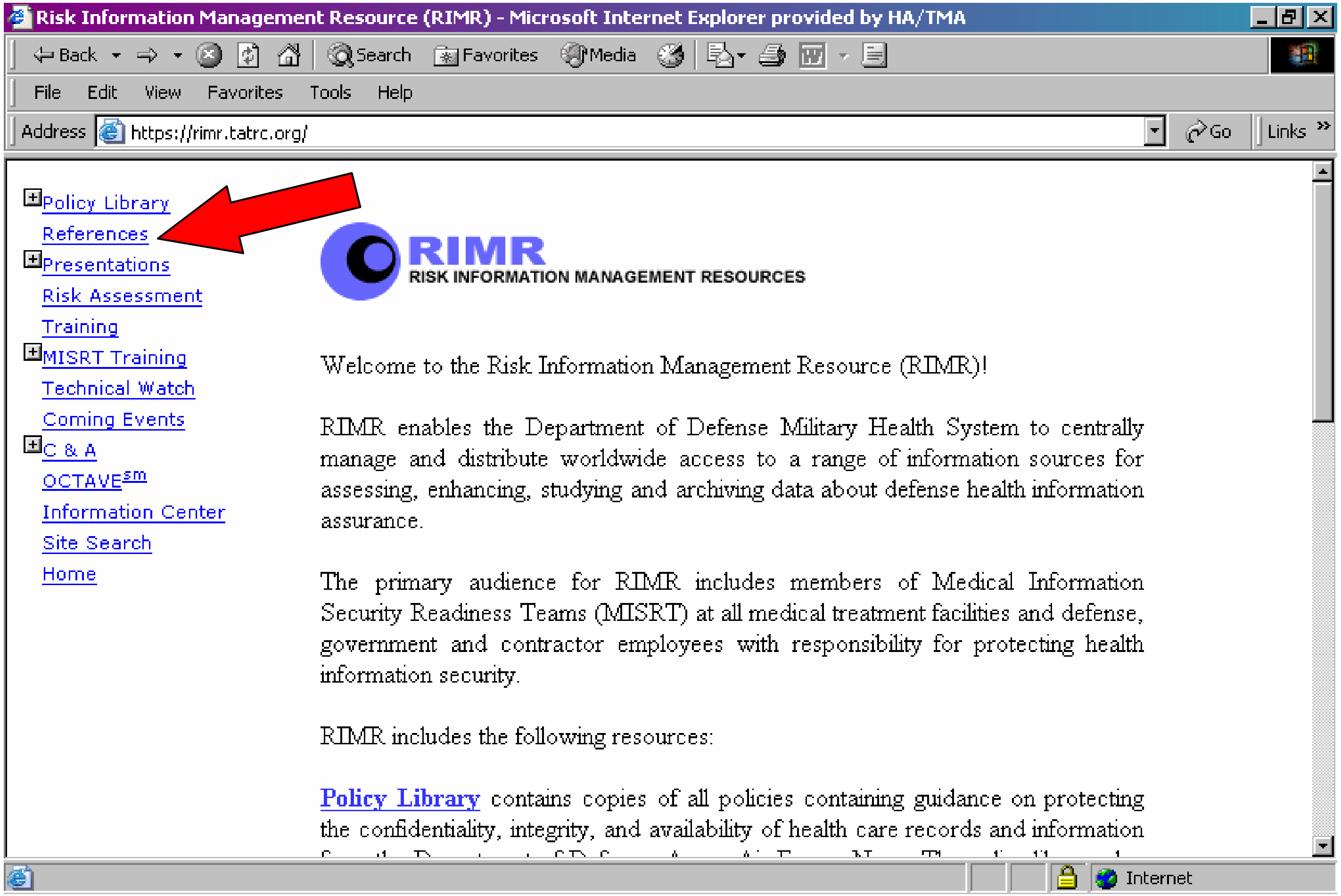
- Report conducted on behalf of the Defense Healthcare Information Assurance Program
- Compares OCTAVE Method to NIST Approach for risk assessment

A Comparison of the
Operationally Critical Threat, Asset and Vulnerability Evaluation ^{SM}
Method
and
Commonly Accepted Best Practices for Assessing Information Security Risks
as stated in the
National Institutes of Standards and Technology Special Publication 800-30
(NIST SP 800-30)

OCTAVE Methodology vs. NIST Risk Management Approach

Report Location (1 of 2)

https://rimr.tatrc.org



Welcome to the Risk Information Management Resource (RIMR)!

RIMR enables the Department of Defense Military Health System to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance.

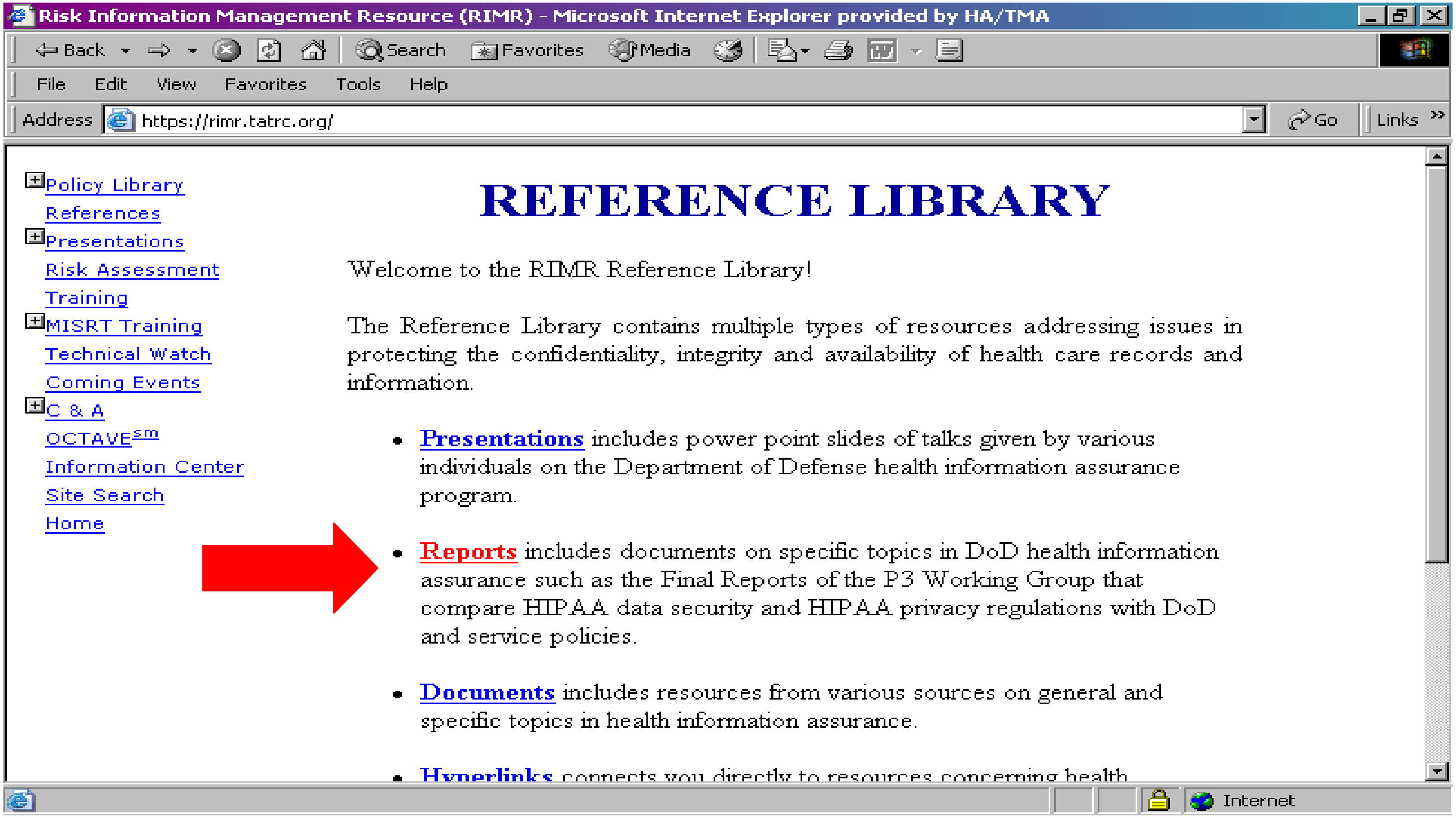
The primary audience for RIMR includes members of Medical Information Security Readiness Teams (MISRT) at all medical treatment facilities and defense, government and contractor employees with responsibility for protecting health information security.

RIMR includes the following resources:

Policy Library contains copies of all policies containing guidance on protecting the confidentiality, integrity, and availability of health care records and information

OCTAVE Methodology vs. NIST Risk Management Approach

Report Location (2 of 2)



- Policy Library
- References
- Presentations
- Risk Assessment
- Training
- MISRT Training
- Technical Watch
- Coming Events
- C & A
- OCTAVE^{sm}
- Information Center
- Site Search
- Home

REFERENCE LIBRARY

Welcome to the RIMR Reference Library!

The Reference Library contains multiple types of resources addressing issues in protecting the confidentiality, integrity and availability of health care records and information.

- **Presentations** includes power point slides of talks given by various individuals on the Department of Defense health information assurance program.
- **Reports** includes documents on specific topics in DoD health information assurance such as the Final Reports of the P3 Working Group that compare HIPAA data security and HIPAA privacy regulations with DoD and service policies.
- **Documents** includes resources from various sources on general and specific topics in health information assurance.
- **Hyperlinks** connects you directly to resources concerning health

OCTAVE Methodology vs. NIST Risk Management Approach

OCTAVE – What is it?

- Operationally Critical Threat, Asset and Vulnerability Evaluation^{SM} Methodology
- Qualitative information risk analysis methodology designed to identify:
  - Information assets critical to the organization or site
  - Threats to those assets
  - Vulnerabilities associated with those information assets
  - Current levels of risk in regard to the security of those critical information assets
- Provides organization of results to facilitate the development of effective and pertinent security protection strategies and risk mitigation plans

OCTAVE

Where did it come from?

- Developed by Carnegie Mellon University and the US Army Medical Research and Materiel Command
  - Part of the Defense Healthcare Information Assurance Program (DHIAP)
- Provided free of cost to the Services
- Training on the OCTAVE Methodology was conducted for all Services during 2001-2003
- Available at: https://dhiapoctave.hcisaac.org/

OCTAVE

Brief Overview

- Activities are conducted before the assessment and in three phases
  - Startup (preparation): Establish analysis team, gather baseline documentation, adapt Catalog or worksheets as needed

OCTAVE

Brief Overview

- Phase 1: Elicit details of asset use and protection
  - Results in Threat Profiles
- Phase 2: Identify infrastructure vulnerabilities
  - Results in Technical Vulnerabilities Summary
- Phase 3: Develop security strategy and plans
  - Results in
    - Organization Protection Strategy
    - Risk Mitigation Plans
    - Action Items
    - Asset Profile Workbooks

NIST Risk Management Approach

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 “Risk Management Guide for Information Technology Systems”
- NIST SP 800-30 provides:
  - Recommendations for the protection of information technology assets by addressing technical and non-technical functions
  - Establishes demonstrable means of managing risk:
    - Risk Assessment
    - Risk Mitigation
    - Risk Monitoring

NIST Risk Assessment Approach

Where did it come from?

- Risk management standard for the government
- Developed by NIST to provide guidance for all Federal agencies to meet Federal Information Security Management Act (FISMA) requirements to:

> Provide information security protections commensurate with risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by the agency or by a contractor of an agency or any other organization on behalf of an agency

NIST Risk Assessment Approach

Brief Overview

- Guidelines and information on the three crucial elements of information risk management
  - Risk Assessment
    - Remember the Nine steps?
      1. System Characterization
      2. Threat Identification
      3. Vulnerability Identification
      4. Control Analysis
      5. Likelihood Determination
      6. Impact analysis
      7. Risk Determination
      8. Control Recommendation
      9. Results Documentation

NIST Risk Assessment Approach

Brief Overview

- Risk Mitigation
  - The most cost-effective approach to implement the most appropriate controls that decrease mission risk to an acceptable level, with minimal adverse impact on the organization’s resources and mission
- Risk Monitoring
  - The continuous monitoring of your systems and processes necessary to keep your organization at the risk level that was deemed acceptable

OCTAVE vs NIST Approach

- Nine steps of the NIST Approach equate to the processes of the OCTAVE Methodology
- Overall comparison
  - NIST provides general guidance on activities that should be accomplished for risk management
  - OCTAVE gives specific details on methods, plans and strategies for managing risk

OCTAVE vs NIST Approach

Three major differences

1. Asset selection process
   - OCTAVE focuses on critical assets only
2. Inclusion of likelihood in risk determination
   - OCTAVE includes no means to factor risk based on likelihood that a particular technical vulnerability may be exploited
3. Quantitative risk assessment guidance
   - OCTAVE provides no guidance on conducting a quantitative information security risk assessment

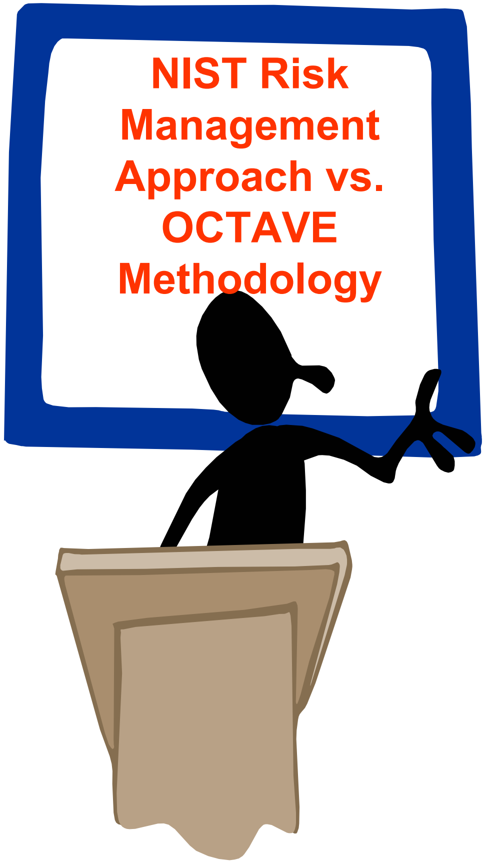
OCTAVE Methodology vs. NIST Risk Management Approach

Bottom Line

- Following the OCTAVE methodology will meet the spirit and intent of the NIST guidance for conducting risk assessment as part of a total risk management program

OCTAVE Methodology vs. NIST Risk Management Approach

Summary



- You should now be able to:
  - Locate the report on *OCTAVE-Best Practices Comparative Analysis*
  - Describe the general phases of the OCTAVE methodology
  - Describe the general steps of the NIST approach
  - Describe how OCTAVE differs from the NIST risk assessment approach
  - Identify common elements between the two methodologies

OCTAVE Support for HIPAA Security

Objectives

- After completing this module, you should be able to:
  - Locate the report on *OCTAVE Support for HIPAA Security/Privacy Standards*
  - Identify the ways that OCTAVE supports HIPAA Security compliance
  - Describe the results of the mapping between OCTAVE and HIPAA security requirements

OCTAVE Support for HIPAA Security

Report

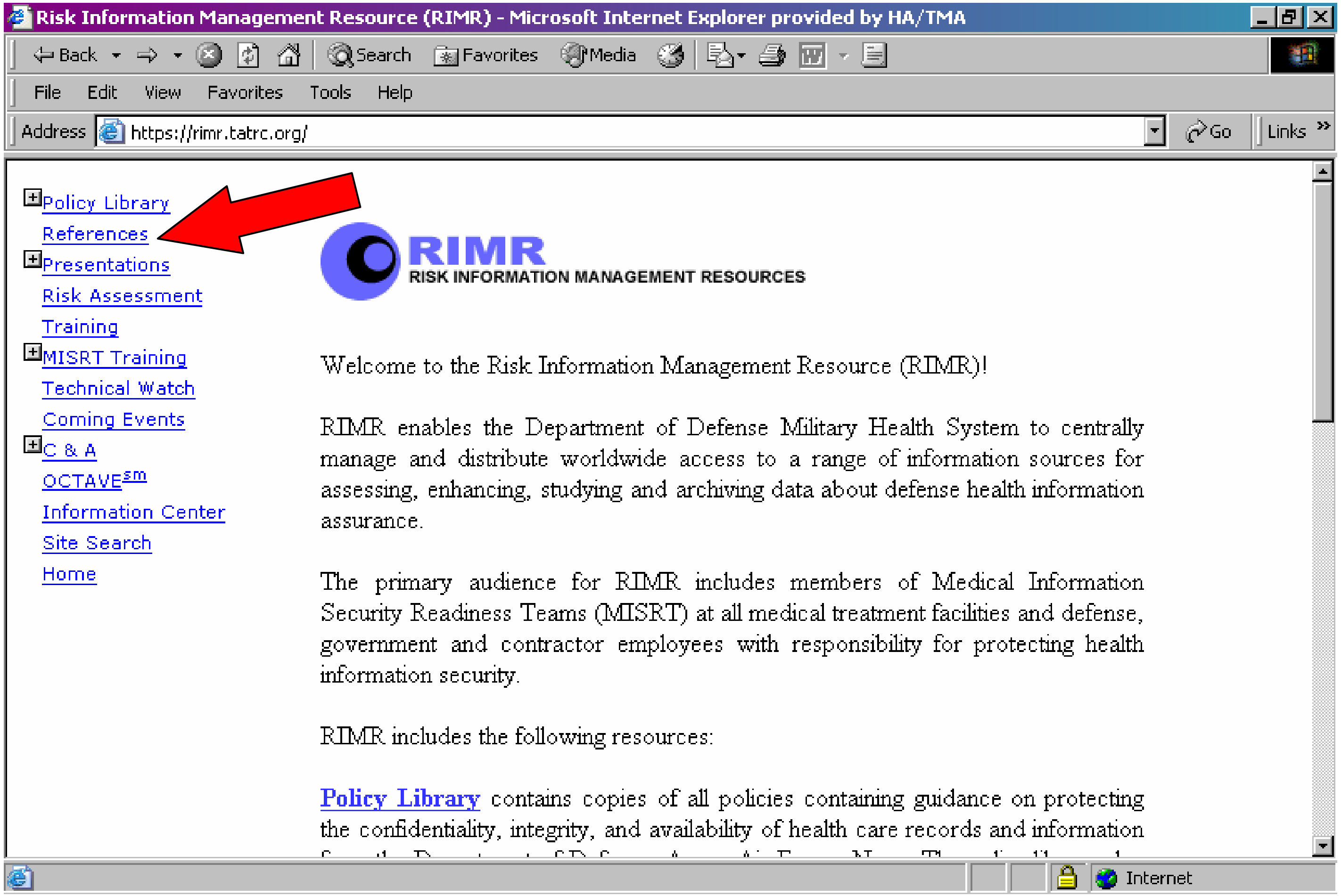
- Report conducted on behalf of the Defense Healthcare Information Assurance Program
- Recommendations for using OCTAVE Method to assist in compliance with HIPAA Rules

Recommendations for Using the
Operationally Critical Threat, Asset and Vulnerability Evaluation^{SM} Method
in Addressing Certain
Health Insurance Portability and Accountability Act of 1196 (HIPAA)
Security and Privacy Standards

OCTAVE Support for HIPAA Security

Report Location (1 of 2)

https://rimr.tatrc.org



Welcome to the Risk Information Management Resource (RIMR)!

RIMR enables the Department of Defense Military Health System to centrally manage and distribute worldwide access to a range of information sources for assessing, enhancing, studying and archiving data about defense health information assurance.

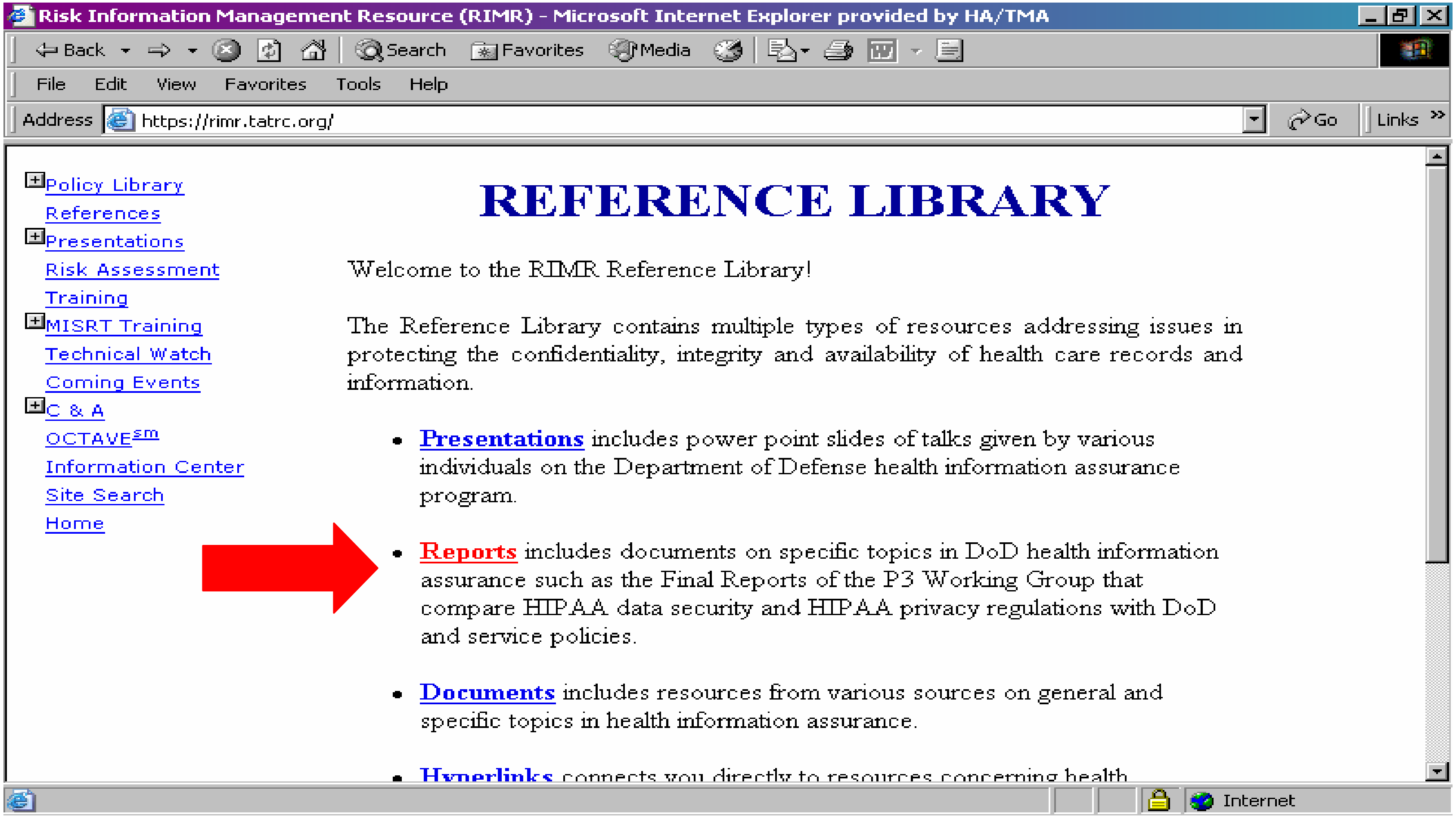
The primary audience for RIMR includes members of Medical Information Security Readiness Teams (MISRT) at all medical treatment facilities and defense, government and contractor employees with responsibility for protecting health information security.

RIMR includes the following resources:

Policy Library contains copies of all policies containing guidance on protecting the confidentiality, integrity, and availability of health care records and information

OCTAVE Support for HIPAA Security

Report Location (2 of 2)



REFERENCE LIBRARY

Welcome to the RIMR Reference Library!

The Reference Library contains multiple types of resources addressing issues in protecting the confidentiality, integrity and availability of health care records and information.

- **Presentations** includes power point slides of talks given by various individuals on the Department of Defense health information assurance program.
- **Reports** includes documents on specific topics in DoD health information assurance such as the Final Reports of the P3 Working Group that compare HIPAA data security and HIPAA privacy regulations with DoD and service policies.
- **Documents** includes resources from various sources on general and specific topics in health information assurance.
- **Hyperlinks** connects you directly to resources concerning health

OCTAVE Support for HIPAA Security

Overview

OCTAVE:

- Risk assessment methodology for critical assets
  - Assumes that critical assets are the site's electronic repositories for PHI
- Helps satisfy most requirements of the HIPAA Security standards by:
  - Following the process
  - Implementing subsequent recommendations
  - Using the strategic and operational practices of the *OCTAVE Catalog of Practices*

OCTAVE Support for HIPAA Security

Results of Mapping

- Appendix B – Detailed Mapping of *OCTAVE Catalog of Practices* to HIPAA Security Standards
- Table 2
  - Shows that OCTAVE provides site with significant support for most of the HIPAA Security Standards

OCTAVE Support for HIPAA Security

Results of Mapping – Table 2

Security Standards Topic	Catalog of Practices Coverage of Security Standards Requirements			Total
	G-Strong Coverage	Y-Some Coverage	R-No Coverage	
Administrative	7 Standards 19 Implementation Specifications	2 Standards	2 Implementation Specifications	30
Physical	4 Standards 7 Implementation Specifications	1 Implementation Specification	======	12
Technical	5 Standards 6 Implementation Specifications	=======	1 Implementation Specification	12
Organizational	=======	=======	7 Standards 19 Implementation Specifications	5
Policies and Procedures	1 Implementation Specification	1 Standard 1 Implementation Specification	1 Standard 1Implementation Specification	5
Total	49	5	10	64
Comment	*54 Covered Strongly/Generally*		*10 Not Covered*	64

Notes: **G**, **Y**, and **R** stand for **G**reen, **Y**ellow and **R**ed

OCTAVE Support for HIPAA Security

Recommended Amendments

- Appendix B – Table 3
  - Provides recommendations on ways to tailor OCTAVE to meet the needs for HIPAA Security
- Next slide is an example of recommended amendments for the Administrative Safeguards

OCTAVE Support for HIPAA Security

Recommended Amendments – Table 3

EVAL	HIPAA Standard or Implementation Specification	Overview of Catalog of Practices (CoP) Coverage of Topic	Recomd
Yellow	Assigned Security Responsibility	The Catalog calls for defining security roles and responsibilities of staff and ensuring responsibility is assigned, but it does not request naming the HIPAA security officer. This requirement could easily be added to SP3.2 and OP3.2.2.	Easy add to CoP
Red	Isolating health care clearinghouse functions	(Note: At that this time, MHS and MTFs do not perform clearinghouse functions, making requirement not applicable to the military environment.38) While the Catalog does address the need to segregate and limit access to authorized individuals, it does not directly address “isolation of health care clearinghouse functions from other functions of the organization.”	n/a for MHS
Yellow	Business associate contracts and other arrangements	The Catalog ascertains whether requirements and procedures for information protection when working with “third parties” exist and are followed. While it does not highlight the specific requirements that HIPAA places on “business associate contracts/other arrangements,” its existing third-party elements indicate the sections of the Catalog that a site might customize in order to directly address the HIPAA requirements.	With care, can be added to CoP
Red	Written contract or other arrangement	The Catalog does not require that arrangements with third parties be documented in writing. If a site has developed the Catalog modifications needed to satisfy 164.308(a)(8)(b)(1), then it would be a minor enhancement to indicate that the agreement must be in writing.	Easy add to CoP

OCTAVE Support for HIPAA Security

Detailed Mapping

- Appendix B – Table 4
  - Analysis includes a detailed one-to-one mapping of each of the HIPAA Security Rule requirements to the OCTAVE practices for the catalog
  - Next slides the level of detail provided in the table

OCTAVE Support for HIPAA Security

Detailed Mapping – Table 3

EXAMPLE: Security Management Process

- Some relevant elements from the OCTAVE *Catalog of Practices*
  - SP2.1 Staff members understand their security roles and responsibilities. This is documented and verified
  - SP2.2 There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified
  - SP2.3 Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization

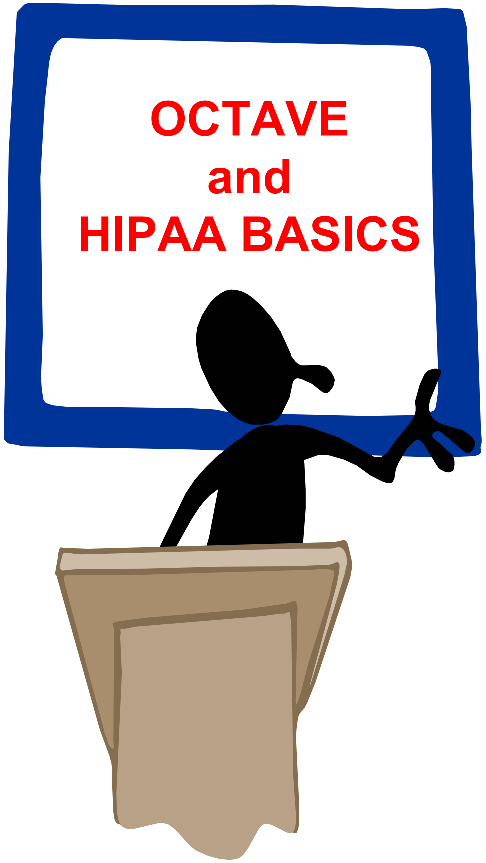
Summary

- You should now be able to:
  - Locate the report on *OCTAVE Support for HIPAA Security/Privacy Standards*
  - Identify the ways that OCTAVE supports HIPAA Security compliance
  - Describe the results of the mapping between OCTAVE and HIPAA security requirements

OCTAVE and HIPAA BASICS

OCTAVE and HIPAA BASICS

Objectives



- After completing this module, you should be able to:
  - Describe the purpose of HIPAA BASICS
  - Identify the differences between OCTAVE and HIPAA BASICS
  - Describe how to utilize both tools to ensure HIPAA security compliance

OCTAVE and HIPAA BASICS

Remember the purpose of OCTAVE?

- Qualitative information risk analysis methodology
- Identifies:
  - Information assets critical to the organization or site
  - Threats to those assets
  - Vulnerabilities associated with those information assets
  - Current levels of risk in regard to the security of those critical information assets

What is HIPAA BASICS?

HIPAA BASICS is:

- Compliance assessment tool specific to HIPAA
- A web-based application
- Used to collect, store, process data and generate reports on HIPAA requirements
- Assists you in identifying where compliance gaps exist and provides suggested compliance activities relating to HIPAA Administrative Simplification

Three Components

- A **Database** containing continually updated information on HIPAA rules, broken down into discrete tasks that must be accomplished in order to achieve HIPAA Compliance

- An **Interface** between your MTF policies and practices and specific HIPAA requirements – enabling the user to clearly see where HIPAA standards are met and where compliance gaps exist

- A **Management Tool** to assign tasks, manage personnel, and monitor progress using customizable reports on compliance status

OCTAVE and HIPAA BASICS

How do they differ?

HIPAA BASICS

- Tool that helps the user design a compliance program, delegate responsibility for compliance tasks, monitor progress, and generate reports
- Tool that anticipates that the user’s desired end state is compliance with all HIPAA standards, including the Security Standards
- Tool to manage HIPAA compliance activities and is limited by the perspective and experience of the individuals completing the process to determine the level of non-compliance risk

OCTAVE

- Risk assessment methodology. Its goal is to assist the user in identifying threats and vulnerabilities, and compare risks
- End state is the completion of a risk assessment and the production of a protection strategy, mitigation plan, and action list
- Encourages consideration of legal requirements (such as health privacy or financial information), but specific HIPAA provisions need to be tailored

OCTAVE and HIPAA BASICS

Complimentary Functions

- Used in combination, HIPAA BASICS and OCTAVE provide a fully integrated approach to security and risk that may extend beyond HIPAA compliance to support the full spectrum of compliance requirements
  - Leveraging of HIPAA BASICS and OCTAVE provides economies of scale for both the security and privacy programs

HIPAA BASICS™

+

octave®

=

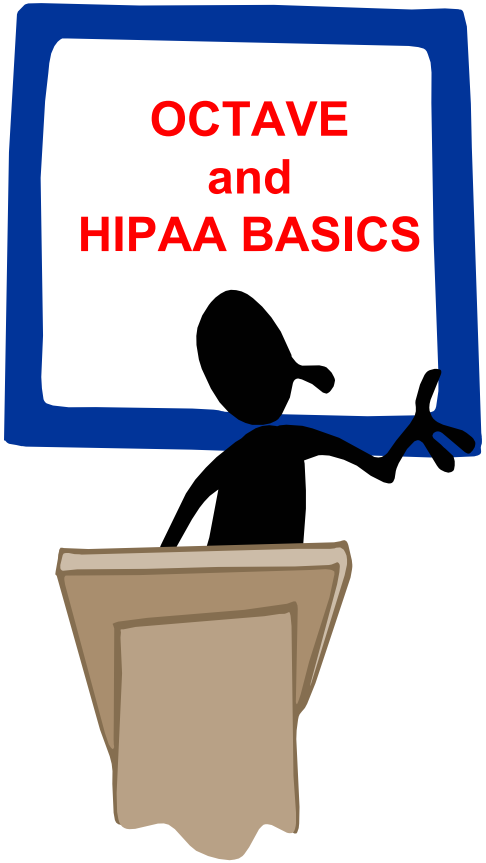
100% HIPAA Compliance

+

Security Program Best Practice

OCTAVE and HIPAA BASICS

Summary



- You should now be able to:
  - Describe the purpose of HIPAA BASICS
  - Identify the differences between OCTAVE and HIPAA BASICS
  - Describe how to utilize both tools to ensure HIPAA security compliance

HIPAA Risk Management Activities

Keys for Success

- Senior management’s commitment
- Full support and participation of the IT team
- Competence of the Risk Assessment team
  - Expertise of applying the risk assessment methodology to the system and the organization
  - Identification of mission risks
  - Provide cost-effective safeguards that meet the need of the organization

HIPAA Risk Management Activities

Keys for Success

- Awareness and cooperation of the user population
  - Follow procedures
  - Comply with implemented controls
- Ongoing evaluation and assessment of the IT related mission risks

HIPAA Risk Management Activities

Summary

- You should now be able to:
  - Define basic information security concepts
  - Describe the elements of the risk management process
  - Identify the risk management activities of the HIPAA Security Rule
  - Describe how OCTAVE and HIPAA BASICS support HIPAA compliance

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA security representatives

Please fill out your critique

Thanks!